IBM SecureWay Trust Authority

Benutzerhandbuch

Version 3 Release 1.2

SH12-2978-01

IBM SecureWay Trust Authority

Benutzerhandbuch

Version 3 Release 1.2

SH12-2978-01

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter „Bemerkungen" auf Seite 49 gelesen werden.

Zweite Ausgabe (Juni 2000)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM SecureWay Trust Authority User's Guide,
IBM Form SH09-4531-01,

herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2000
© Copyright IBM Deutschland Informationssysteme GmbH 2000

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW NLS Center
Kst. 2877
Juni 2000

Inhaltsverzeichnis

Kapitel 1. Produktinformationen zu Trust Authority 1

Kapitel 2. Übersicht 3

Kapitel 3. Informationen zur Vorgehensweise 5

Zugriff auf die Registrierungs-Web-Seite 5
Registrierung über einen Browser 5
Ein Browser-Zertifikat anfordern 6
Einen Server oder eine Einheit registrieren . . . 7
Eine Person vorab registrieren 9
Den Registrierungsstatus überprüfen 10
Verwaltung von Zertifikaten unter Verwendung eines Browsers 11
Ein Zertifikat in den Wartestatus setzen 12
Ein Zertifikat erneuern 12
Ein Zertifikat widerrufen 13
Aktive Anforderungen abbrechen 14
Mit mehreren Zertifikaten arbeiten 14
Client-Anwendung installieren 14
Physische Smart Cards aktivieren 15
Die Client-Anwendung aufrufen 16
Über den Client registrieren 17
Registrierung unter Verwendung einer Vorabregistrierungsdatei 17
Registrierung unter Verwendung einer Transaktions-ID 17
Verwaltung von Zertifikaten unter Verwendung des Client 18
Ein Zertifikat oder eine anstehende Anforderung löschen 18
Ein Zertifikat von einer Smart Card in eine Datei exportieren 18
Ein Zertifikat aus einer Datei auf eine Smart Card importieren 19
Ein Zertifikat auf eine andere Smart Card verschieben 19
Ein Zertifikat zum Anzeigen von Details öffnen 19
Ein Zertifikat in den Wartestatus setzen 20
Ein Zertifikat erneuern 20
Demnächst ablaufende Zertifikate erneuern. . . 20
Ein Zertifikat widerrufen 21
Dateien unterzeichnen 21
Mit einer Zertifikatliste arbeiten 22
Zwischen Registerkarten wechseln. 22
Mehr Zeilen in einer Tabelle anzeigen 22
Die Größe einer Tabellenspalte ändern 23
Verwaltung von Smart Cards unter Verwendung des Client 23
Eine andere Smart Card öffnen 23
Ein Smart Card-Kennwort ändern 23
Smart Card-Eigenschaften anzeigen 24
Client-Anwendung verlassen 24
Client-Anwendung deinstallieren 24

Kapitel 4. Erläuterungen 25

Registrierung 25
Vorabregistrierung 25
Web-Browser-Unterstützung 26
Registrierung 26
Unternehmensregeln 26
Registrierungsstellen (RAs) 27
Registrierungsdatenbanken 27
Registrierungsdomänen 27
Registrierungssätze 28
Datensatzeigenschaften 28
Zertifizierung. 28
Zertifikatsaussteller 28
Zertifikatswiderrufslisten (CRL) 28
Verzeichnisse 28
Registrierter Name 29
Zertifikate 29
Browser-Zertifikate 29
CA-Zertifikate 29
Server- und Einheitenzertifikate 30
Zertifikatserweiterungen 30
Zertifikatsverarbeitungszyklus 30
Erneuerbarkeit 30
Zugriff auf gesicherte Ressourcen 31
Zugriffssteuerung 31
Authentifizierung und Genehmigung. 31
Digitale Unterschriften 31
Smart Cards 31

Kapitel 5. Referenzinformationen . . . 33

Registrierungsformular auf der Web-Seite 33
Verfügbare Zertifikatstypen 36
Begründung für den Widerruf von Zertifikaten . . 37
Systemvoraussetzungen für die Browser-Registrierung 38
Systemvoraussetzungen für die Client-Anwendung 38
Client-Anwendung - Hauptfenster. 39
Menüs im Fenster 'Smart Card'. 39
Registerkarten im Fenster 'Smart Card' 40
Tabellen im Fenster 'Smart Card' 40
Dialoge der Client-Anwendung. 40
Dialog 'Zertifikatserneuerung' 41
Dialog 'Kennwort ändern' 41
Dialog 'Zertifikat löschen' 41
Dialog 'Zertifikat exportieren' 42
Dialog 'Zertifikat importieren' 42
Dialog 'Neues Zertifikat unter Verwendung einer Vorabregistrierungsdatei' 42
Dialog 'Neues Zertifikat unter Verwendung einer Transaktions-ID' 43
Dialog 'Zertifikat öffnen' 43
Dialog 'Smart Card öffnen' 44
Dialog 'Zertifikat erneuern' 45
Dialog 'Zertifikat widerrufen' 45
Dialog 'Datei unterzeichnen'. 46

Dialog 'Smart Card-Eigenschaften'. 46
Hilfe für die Client-Anwendung 47
Überlegungen zur Unterstützung in der Landessprache 47

Bemerkungen 49
Marken und Dienstleistungsmarken 50

Bezugsinformationen 53

Glossar 55

Index 69

Kapitel 1. Produktinformationen zu Trust Authority

IBM SecureWay stellt Anwendungen zur Verfügung, mit denen Benutzer authentifiziert werden können und die eine sichere Datenfernverarbeitung gewährleisten.

- Das Produkt ermöglicht es Unternehmen, digitale Zertifikate in Übereinstimmungen mit ihren Regeln zur Registrierung und Zertifizierung auszustellen, zu veröffentlichen und zu verwalten.
- Die Unterstützung von Public Key Infrastructure für X.509 Version 3 (PKIX) und CDSA-Verschlüsselungsstandards (Common Data Security Architecture) ermöglicht die Interoperabilität zwischen Produkten verschiedener Hersteller.
- Mit Hilfe von digitalen Unterschriften und sicheren Protokollen ist es möglich, alle Parteien einer Transaktion zu authentifizieren.
- Registrierungsfunktionen auf Browser- und Client-Basis bieten maximale Flexibilität.
- Die verschlüsselte Datenfernverarbeitung und die sichere Speicherung von Registrierungsinformationen sorgen für ein hohes Maß an Vertraulichkeit.

Ein Trust Authority-System kann auf IBM AIX/6000- und Microsoft Windows NT-Server-Plattformen ausgeführt werden. Es bietet die folgenden Hauptfunktionen:

- Ein zuverlässiger Zertifikatsaussteller (CA) verwaltet den gesamten Verarbeitungszyklus der digitalen Zertifizierung. Um für die Authentizität eines Zertifikats zu garantieren, versieht der CA jedes ausgestellte Zertifikat mit einer digitalen Unterschrift. Er unterzeichnet auch Zertifikatswiderrufslisten (CRLs), um zu gewährleisten, daß bestimmte Zertifikate nicht mehr gültig sind. Zur weiteren Sicherung seines Unterschriftsschlüssels können sie kryptografische Hardware wie beispielsweise den IBM SecureWay 4758 PCI Cryptographic Coprocessor verwenden.
- Eine Registrierungsstelle (RA) führt die administrativen Tasks im Hintergrund der Benutzerregistrierung aus. Die RA stellt sicher, daß nur solche Zertifikate ausgestellt werden, die Ihre Geschäftstätigkeit unterstützen, und daß diese Zertifikate ausschließlich an berechtigte Benutzer ausgegeben werden. Die administrativen Tasks können von automatisierten Prozessen ausgeführt werden oder von Mitarbeitern, die entsprechende Entscheidungen treffen.
- Eine Registrierungsschnittstelle auf Web-Basis sorgt dafür, daß Zertifikate für Browser, Server und andere Zwecke wie beispielsweise für VPN-Einheiten (Virtual Private Network), Smart Cards und sichere E-Mail-Übertragung ohne Schwierigkeiten abgerufen werden können.
- Eine Windows-Anwendung, der Trust Authority-Client, ermöglicht Endbenutzern das Abrufen und Verwalten von Zertifikaten ohne einen Web-Browser.
- Eine Verwaltungsschnittstelle auf Web-Basis, der RA Desktop, ermöglicht es berechtigten Registrierern, Registrierungsanforderungen zu genehmigen oder zurückzuweisen und Zertifikate nach dem Ausstellen zu verwalten.
- Ein Protokollierungssubsystem berechnet für jeden Protokolleintrag einen Nachrichtenauthentifizierungscode (MAC, Message Authentication Code). Wenn die Protokolldaten geändert oder gelöscht werden, nachdem sie in die Protokolldatenbank geschrieben wurden, können Sie diesen Eingriff anhand des MAC feststellen.
- Regel-Exits ermöglichen es den Anwendungsentwicklern, die Registrierungsprozesse anzupassen.

- Integrierte Unterstützung für eine Steuerkomponente zur Verschlüsselung. Damit Operationen im Rahmen der Datenfernverarbeitung authentifiziert werden können, werden die Hauptkomponenten von Trust Authority mit einem werkseitig erstellten privaten Schlüssel unterzeichnet. Sicherheitsobjekte wie beispielsweise Schlüssel und MACs werden verschlüsselt und in geschützten Bereichen, den sogenannten KeyStores (Schlüsselspeichern), aufbewahrt.
- Integrierte Unterstützung für IBM SecureWay Directory. Das Directory speichert Informationen zu gültigen und widerrufenen Zertifikaten in einem LDAP-kompatiblen Format (LDAP = Lightweight Direct Access Protocol).
- Integrierte Unterstützung für IBM WebSphere Application Server und IBM HTTP Server. Der Web-Server arbeitet mit dem RA-Server zusammen, um Nachrichten zu verschlüsseln, Anforderungen zu authentifizieren und Zertifikate an den vorgesehenen Empfänger zu senden.
- Integrierte Unterstützung für das ausgezeichnete IBM Produkt IBM DB2 Universal Database.

Kapitel 2. Übersicht

Wenn die gesicherten Anwendungen eines Unternehmens durch Trust Authority geschützt werden, können ausschließlich Benutzer mit entsprechenden Berechtigungen auf diese Anwendungen zugreifen. Wer eine Berechtigung wie beispielsweise ein digitales Zertifikat benötigt, kann diese anfordern, indem er bestimmte Informationen zur Verfügung stellt. Die Daten in der Registrierungsanforderung stellen die Grundlage für die Entscheidung dar, ob die Anforderung genehmigt oder zurückgewiesen wird. Wenn eine Registrierungsanforderung genehmigt wird, bearbeitet die Trust Authority-Registrierungsstelle (Registration Authority, RA) die Anforderung und der Trust Authority- Zertifikatsaussteller (Certificate Authority, CA) stellt das Zertifikat aus. Die Datensätze der Registrierungsanforderungen und Zertifikate befinden sich in einer verschlüsselten Registrierungsdatenbank.

Ein Trust Authority-System bietet mehrere Möglichkeiten zum Anfordern eines Zertifikats:

- Die Trust Authority-Registrierungsformulare, die auf einer Web-Seite zur Verfügung stehen.
- Die Trust Authority-Client-Anwendung, die unter Microsoft Windows ausgeführt wird.

Ihr Unternehmen kann entweder eine der beiden Methoden verwenden oder auch beide zusammen, je nachdem, was die Mitarbeiter, die sich registrieren wollen, bevorzugen, und was am besten im Hinblick auf die Unternehmensregeln geeignet ist.

Mit Hilfe der Registrierungsformulare können Sie die für die Anforderung eines Zertifikats erforderlichen Informationen übergeben und später zum Formular zurückkehren, um die Antwort der Trust Authority-Registrierungsfunktion abzurufen. Sie können ein Browser-Zertifikat, ein Server-Zertifikat oder ein Einheitenzertifikat beantragen. Sie haben auch die Möglichkeit, sich für ein Zertifikat vorab registrieren zu lassen, das den Zugriff auf PKIX-kompatible Anwendungen ermöglicht. Sie haben ebenfalls die Möglichkeit, zur Registrierungs-Web-Seite zurückzukehren, um die von dort direkt empfangenen Zertifikate zu verwalten.

Die Client-Anwendung bietet einen vereinfachten Prozeß, der für Benutzer gedacht ist, die sich bereits vorab registriert haben. Die Anwendung stellt auch Dialoge und Befehle zur Verfügung, die Ihnen dabei helfen sollen, Ihre Zertifikate abzurufen und anschließend zu verwalten.

Das vorliegende Handbuch unterstützt Sie bei allen genannten Registrierungs-Tasks.

Kapitel 3. Informationen zur Vorgehensweise

Die folgenden Abschnitte enthalten:

- Anweisungen zu jedem Schritt bei der Registrierung eines Zertifikats auf der Registrierungs-Web-Seite von Trust Authority sowie Anweisungen dazu, wie Sie diese Seite verwenden, um die dort abgerufenen Browser-Zertifikate zu verwalten.
- Anweisungen dazu, wie die Trust Authority-Client-Anwendung verwendet wird, um ein Zertifikat nach der Vorabregistrierung anzufordern oder um Ihre Zertifikate zu verwalten und zu verwenden.

Zugriff auf die Registrierungs-Web-Seite

Um auf die Registrierungs-Web-Seite zuzugreifen, gehen Sie folgendermaßen vor:

1. Stellen Sie sicher, daß Ihre Datenstation die im Abschnitt „Systemvoraussetzungen für die Browser-Registrierung" auf Seite 38 aufgeführten Anforderungen erfüllt.
2. Rufen Sie die URL Ihres Unternehmens für den Zugriff auf die Registrierungs-Web-Seite ab. Die URL hat das folgende Format:

   `http://`*`Mein_öffentlicher_Web-Server`*`/`*`Meine_Domäne`*`/index.jsp`
3. Öffnen Sie Ihren Browser, und geben Sie die URL ein:
   - Wenn Sie Netscape verwenden, geben Sie die URL bei **Pfad** in das Textfenster ein.
   - Wenn Sie den Internet Explorer verwenden, geben Sie die URL bei **Adresse** in das Textfenster ein.
4. Drücken Sie die **Eingabetaste**.

   Die Registrierungs-Web-Seite von Trust Authority wird angezeigt. Bei einer Standardinstallation lautet der Name der Seite 'Identitätsnachweis - Verwaltung'.
5. Wenn Sie die Trust Authority-Registrierungsservices das erste Mal verwenden, klicken Sie auf **das Zertifikat für Ihren Server**.

   Mit diesem Zertifikat kann Ihr Browser Daten authentifizieren, die von den Registrierungsservices gesendet werden. Wenn Sie diese Services das nächste Mal verwenden, können Sie diesen Schritt übergehen.

Registrierung über einen Browser

In diesem Abschnitt wird beschrieben, wie Sie Ihren Web-Browser verwenden, um ein Zertifikat auf der Trust Authority-Registrierungsseite anzufordern.

Wenn Sie die Registrierungsservices das erste Mal verwenden, müssen Sie ein CA-Zertifikat für Ihren Web-Browser abrufen, bevor Sie fortfahren können. Anschließend können Sie die Seiten zur Registrierung wiederholt verwenden.

Abhängig davon, wie die Registrierungsfunktion für Ihr Unternehmen angepaßt wurde, können die Prozeduren, die zum Abrufen eines gültigen Zertifikats ausgeführt werden müssen, unterschiedlich sein. Im folgenden werden die grundlegenden Schritte erklärt. Wenden Sie sich an den zuständigen Systemadministrator, um Informationen über die für Ihren Standort gültigen Prozeduren zu erhalten.

Ein Browser-Zertifikat anfordern

Um ein Browser-Zertifikat über Ihren Web-Browser abzurufen, gehen Sie folgendermaßen vor:

1. Nehmen Sie über Ihren Browser Zugriff auf die Registrierungs-Web-Seite.
2. Öffnen Sie über **Registrierungsart** die Liste, und wählen Sie **Browser-Zertifikat aus.**
3. Wählen Sie über **Aktion** die Option **Registrieren** aus.
4. Klicken Sie auf **OK**.

   Das angeforderte Registrierungsformular wird angezeigt.
5. Befolgen Sie die Anweisungen auf der Web-Seite, um die Felder des Formulars auszufüllen. Im Abschnitt „Registrierungsformular auf der Web-Seite" auf Seite 33 werden die Felder beschrieben. Das Formular enthält die folgenden Abschnitte:
   - Einen Abschnitt für die **Registrierungsinformationen** mit Textfenstern, in die Sie die Informationen zu Ihrer Person eingeben.
   - Einen Abschnitt für die **Zertifikatsanforderungsinformationen** mit Textfenstern, in die Sie die Informationen über das gewünschte Zertifikat eingeben. Wenn Sie in die Kanneingabefelder des jeweiligen Abschnitts keine Werte eintragen, setzt Trust Authority Standardwerte ein, die dem von Ihnen angeforderten Zertifikatstyp zugeordnet sind.

   Bitte achten Sie insbesondere auf die folgenden Felder:

   Zertifikatstyp
   Wählen Sie die Art des Browser-Zertifikats aus, das Sie für Ihr Unternehmen abrufen sollen. Im Abschnitt „Verfügbare Zertifikatstypen" auf Seite 36 werden die Zertifikatstypen beschrieben.

   CA-Zertifikat auf Browser installieren
   Klicken Sie hier, um ein entsprechendes CA-Zertifikat abzurufen, das mit dem Zertifikatstyp vereinbar ist. Wenn Sie diesen Knopf anklicken, wird das CA-Zertifikat sofort heruntergeladen.

   Mit diesem Zertifikat kann Ihr Browser Daten authentifizieren, die von Trust Authority gesendet werden. Wenn Sie aus irgendeinem Grund bereits über ein solches Zertifikat verfügen, benötigen Sie davon kein zweites.

   E-Mail-Adresse
   Um **E-Mail-Benachrichtigung** auswählen zu können, müssen Sie Ihre E-Mail-Adresse angeben.

   E-Mail-Benachrichtigung
   Wählen Sie dieses Feld aus, wenn Sie per E-Mail über das Ergebnis Ihrer Anforderung benachrichtigt werden wollen.

   Identifikationsprüfungsantwort
   Stellen Sie sicher, daß Sie die von Ihnen angegebene **Identifikationsprüfungsantwort** (von Groß-/Kleinschreibung abhängig) nicht vergessen. Sie benötigen die Antwort später, um den Status der Registrierungsanforderung überprüfen zu können.

   Allgemeiner Name
   Das Feld **Allgemeiner Name** enthält bereits Informationen, die Sie für **Vorname** und **Nachname** angeben. Wenn Sie die Einträge für den Vor- bzw. Nachnamen zu einem späteren Zeitpunkt ändern, werden diese Änderungen möglicherweise nicht automatisch für den allgemeinen

Namen übernommen. Ist dies der Fall, müssen Sie das Feld **Allgemeiner Name** mit dem geänderten **Vornamen** und **Nachnamen** aktualisieren, bevor Sie das Registrierungsformular übergeben.

Domänenname
Geben Sie den Namen der Maschine an, auf der das Zertifikat installiert wird, falls sie mit der Verwendung des Zertifikats in Zusammenhang steht. Für Browser-Zertifikate ist dieses Feld wahlfrei. Verwenden Sie das Feld nur, wenn Sie dazu entsprechende Anweisungen erhalten haben.

6. Klicken Sie auf **Registrierungsanforderung übergeben**.

   Nachdem Trust Authority das Registrierungsformular erhalten hat, geschieht folgendes:

   - Wenn das Formular Fehler enthält, werden diese Fehler angezeigt. Nehmen Sie die entsprechenden Änderungen vor, und klicken Sie auf **Registrierungsanforderung erneut übergeben**.
   - Wenn das Formular keine Fehler enthält, wird ihre Anforderungs-ID auf einer anderen Web-Seite angezeigt.

7. Sie sollten Ihre Anforderungs-ID auf jeden Fall notieren. Sie dient später zu Ihrer Identifizierung, damit Sie den Status der Anforderung überprüfen können und Ihr Zertifikat nach dessen Fertigstellung erhalten. Führen Sie einen der folgenden Schritte aus, wie auf der Web-Seite beschrieben:

   - Markieren Sie die Web-Seite mit einem Lesezeichen, damit Sie ohne Schwierigkeiten zu dieser Anzeige zurückkehren und den Status Ihres Zertifikats überprüfen können.
   - Notieren Sie die Anforderungs-ID, damit Sie diese angeben können, wenn Sie zurückkehren.
   - Warten Sie, bis Ihnen die Anforderungs-ID per E-Mail zugesandt wird.

Einen Server oder eine Einheit registrieren

Alle Server und Einheiten, die Sie registrieren, müssen über spezifische Merkmale verfügen, die den Definitionen dieses Handbuchs entsprechen. Im Abschnitt „Server- und Einheitenzertifikate" auf Seite 30 werden diese Merkmale beschrieben.

Um ein Server- oder Einheitenzertifikat über Ihren Web-Browser abzurufen, gehen Sie folgendermaßen vor:

1. Nehmen Sie über Ihren Browser Zugriff auf die Registrierungs-Web-Seite.
2. Öffnen Sie über **Registrierungsart** die Liste, und wählen Sie **Server- oder Einheitenzertifikat** aus.
3. Wählen Sie über **Aktion** die Option **Registrieren** aus.
4. Klicken Sie auf **OK**.

   Das angeforderte Registrierungsformular wird angezeigt.

5. Befolgen Sie die Anweisungen auf der Web-Seite, um die Felder des Formulars auszufüllen. Im Abschnitt „Registrierungsformular auf der Web-Seite" auf Seite 33 werden die Felder beschrieben. Das Formular enthält die folgenden Abschnitte:

   - Einen Abschnitt für die **Registrierungsinformationen** mit Textfenstern, in die Sie die Informationen zu Ihrer Person eingeben.
   - Einen Abschnitt für die **Zertifikatsanforderungsinformationen** mit Textfenstern, in die Sie die Informationen über das für den Server oder die Einheit gewünschte Zertifikat eingeben. Wenn Sie in die Kanneingabefelder des

jeweiligen Abschnitts keine Werte eintragen, setzt Trust Authority Standardwerte ein, die dem von Ihnen angeforderten Zertifikatstyp zugeordnet sind.

Bitte achten Sie insbesondere auf die folgenden Felder:

Zertifikatstyp
Wählen Sie die Art des Server- oder Einheitenzertifikats aus, das Sie für Ihr Unternehmen anfordern sollen. Im Abschnitt „Verfügbare Zertifikatstypen" auf Seite 36 werden die Zertifikatstypen beschrieben.

CA-Zertifikat in Datei sichern
Klicken Sie hier, um ein entsprechendes CA-Zertifikat abzurufen, das mit dem Zertifikatstyp vereinbar ist. Ihr Browser fordert Sie auf, einen Pfad einzugeben. Wenn Sie diesen Knopf anklicken, wird das CA-Zertifikat sofort heruntergeladen.

Mit diesem Zertifikat kann der Server oder die Einheit Daten authentifizieren, die von Trust Authority gesendet werden. Wenn Sie aus irgendeinem Grund bereits über ein solches Zertifikat verfügen, benötigen Sie davon kein zweites.

E-Mail-Adresse
Um **E-Mail-Benachrichtigung** auswählen zu können, müssen Sie Ihre E-Mail-Adresse angeben.

E-Mail-Benachrichtigung
Wählen Sie dieses Feld aus, wenn Sie per E-Mail über das Ergebnis Ihrer Anforderung benachrichtigt werden wollen.

Identifikationsprüfungsantwort
Stellen Sie sicher, daß Sie die von Ihnen angegebene **Identifikationsprüfungsantwort** (von Groß-/Kleinschreibung abhängig) nicht vergessen. Sie benötigen die Antwort später, um den Status der Registrierungsanforderung überprüfen zu können.

Allgemeiner Name
Das Feld **Allgemeiner Name** enthält bereits Informationen, die Sie für **Vorname** und **Nachname** angeben. Wenn Sie die Einträge für den Vor- bzw. Nachnamen zu einem späteren Zeitpunkt ändern, werden diese Änderungen möglicherweise nicht automatisch für den allgemeinen Namen übernommen. Ist dies der Fall, müssen Sie das Feld **Allgemeiner Name** mit dem geänderten **Vornamen** und **Nachnamen** aktualisieren, bevor Sie das Registrierungsformular übergeben.

Domänenname
Geben Sie den Namen der Maschine an, auf der das Zertifikat installiert wird, falls sie mit der Verwendung des Zertifikats in Zusammenhang steht. Für Server-Zertifikate ist dieses Feld wahlfrei. Wenn Sie es verwenden, identifizieren Sie die Maschine, auf der der Web-Server installiert ist. Der **Domänenname** ist für IPSec-Zertifikate erforderlich. Sie müssen die IPSec-Einheit identifizieren, auf der das Zertifikat installiert wird.

6. Klicken Sie auf **Registrierungsanforderung übergeben**.

   Nachdem Trust Authority das Registrierungsformular erhalten hat, geschieht folgendes:

   - Wenn das Formular Fehler enthält, werden diese Fehler angezeigt. Nehmen Sie die entsprechenden Änderungen vor, und klicken Sie auf **Registrierungsanforderung erneut übergeben**.

- Wenn das Formular keine Fehler enthält, wird ihre Anforderungs-ID auf einer anderen Web-Seite angezeigt.

7. Sie sollten Ihre Anforderungs-ID auf jeden Fall notieren. Sie dient später zu Ihrer Identifizierung, damit Sie den Status der Anforderung überprüfen können und Ihr Zertifikat nach dessen Fertigstellung erhalten. Führen Sie einen der folgenden Schritte aus, wie auf der Web-Seite beschrieben:
   - Markieren Sie die Web-Seite mit einem Lesezeichen, damit Sie ohne Schwierigkeiten zu dieser Anzeige zurückkehren und den Status Ihres Zertifikats überprüfen können.
   - Notieren Sie die Anforderungs-ID, damit Sie diese angeben können, wenn Sie zurückkehren.
   - Warten Sie, bis Ihnen die Anforderungs-ID per E-Mail zugesandt wird.

Eine Person vorab registrieren

Sie können die Registrierungsservices verwenden, um sich selbst oder eine andere Person vorab für ein Zertifikat zu registrieren, mit dem auf eine PKIX-kompatible Anwendung zugegriffen werden kann. Das Zertifikat kann zu einem späteren Zeitpunkt heruntergeladen werden, während die Trust Authority-Client-Anwendung verwendet wird.

Um eine Person über den Web-Browser vorab zu registrieren, gehen Sie folgendermaßen vor:

1. Nehmen Sie über Ihren Browser Zugriff auf die Registrierungs-Web-Seite.
2. Öffnen Sie über **Registrierungsart** die die Liste, und wählen Sie **Vorabregistrierung von Zertifikaten** aus.
3. Wählen Sie über **Aktion** die Option **Registrieren** aus.
4. Klicken Sie auf **OK**.

   Das angeforderte Registrierungsformular wird angezeigt.
5. Befolgen Sie die Anweisungen auf der Web-Seite, um die Felder des Formulars auszufüllen. Im Abschnitt „Registrierungsformular auf der Web-Seite" auf Seite 33 werden die Felder beschrieben. Das Formular enthält die folgenden Abschnitte:
   - Einen Abschnitt für die **Registrierungsinformationen** mit Textfenstern, in die Sie die Informationen über die Person eingeben, die Sie vorab registrieren wollen. An dieser Stelle geben Sie auch einige Informationen ein, anhand deren Sie den Status Ihrer Anforderung überprüfen können.
   - Einen Abschnitt für die **Zertifikatsanforderungsinformationen** mit Textfenstern, in die Sie die Informationen über das gewünschte Zertifikat eingeben. Wenn Sie in die Kanneingabefelder des jeweiligen Abschnitts keine Werte eintragen, setzt Trust Authority Standardwerte ein, die dem von Ihnen angeforderten Zertifikatstyp zugeordnet sind.

   Bitte achten Sie insbesondere auf die folgenden Felder:

   Zertifikatstyp
   Wählen Sie den Zertifikatstyp aus, den die Person, die Sie vorab registrieren, benötigt. Im Abschnitt „Verfügbare Zertifikatstypen" auf Seite 36 werden die Zertifikatstypen beschrieben.

   E-Mail-Adresse
   Um **E-Mail-Benachrichtigung** auswählen zu können, müssen Sie Ihre eigene E-Mail-Adresse angeben.

E-Mail-Benachrichtigung
Wählen Sie dieses Feld aus, wenn Sie per E-Mail über das Ergebnis Ihrer Anforderung benachrichtigt werden wollen.

Identifikationsprüfungsantwort
Stellen Sie sicher, daß Sie die von Ihnen angegebene **Identifikationsprüfungsantwort** (von Groß-/Kleinschreibung abhängig) nicht vergessen. Sie benötigen die Antwort später, um den Status der Registrierungsanforderung überprüfen zu können.

Allgemeiner Name
Das Feld **Allgemeiner Name** enthält bereits Informationen, die Sie für **Vorname** und **Nachname** angeben. Wenn Sie die Einträge für den Vor- bzw. Nachnamen zu einem späteren Zeitpunkt ändern, werden diese Änderungen möglicherweise nicht automatisch für den allgemeinen Namen übernommen. Ist dies der Fall, müssen Sie das Feld **Allgemeiner Name** mit dem geänderten **Vornamen** und **Nachnamen** aktualisieren, bevor Sie das Registrierungsformular übergeben.

Domänenname
Geben Sie den Namen der Maschine an, auf der das Zertifikat installiert wird, falls sie mit der Verwendung des Zertifikats in Zusammenhang steht. Für Vorabregistrierungszertifikate ist dieses Feld wahlfrei. Verwenden Sie das Feld nur, wenn Sie dazu entsprechende Anweisungen erhalten haben.

6. Klicken Sie auf **Registrierungsanforderung übergeben**.

   Nachdem Trust Authority das Registrierungsformular erhalten hat, geschieht folgendes:

   - Wenn das Formular Fehler enthält, werden diese Fehler angezeigt. Nehmen Sie die entsprechenden Änderungen vor, und klicken Sie auf **Registrierungsanforderung erneut übergeben**.
   - Wenn das Formular keine Fehler enthält, wird ihre Anforderungs-ID auf einer anderen Web-Seite angezeigt.

7. Sie sollten Ihre Anforderungs-ID auf jeden Fall notieren. Sie dient später zu Ihrer Identifizierung, damit Sie den Status der Anforderung überprüfen können und Ihr Zertifikat nach dessen Fertigstellung erhalten. Führen Sie einen der folgenden Schritte aus, wie auf der Web-Seite beschrieben:

   - Markieren Sie die Web-Seite mit einem Lesezeichen, damit Sie ohne Schwierigkeiten zu dieser Anzeige zurückkehren und den Status Ihres Zertifikats überprüfen können.
   - Notieren Sie die Anforderungs-ID, damit Sie diese angeben können, wenn Sie zurückkehren.
   - Warten Sie, bis Ihnen die Anforderungs-ID per E-Mail zugesandt wird.

Den Registrierungsstatus überprüfen

Um den Status Ihrer Registrierungsanforderung zu überprüfen, müssen Sie entweder zur der Web-Seite zurückkehren, die Sie während der Registrierung mit einem Lesezeichen markiert haben, oder die folgenden Schritte ausführen:

1. Nehmen Sie Zugriff auf die Registrierungs-Web-Seite.
2. Wählen Sie über **Registrierungsart** den Typ der von Ihnen angeforderten Registrierung aus.
3. Wählen Sie über **Aktion** die Option **Status überprüfen** aus.
4. Klicken Sie auf **OK**.

Die Anzeige enthält Felder, in denen Sie Ihre Identität authentifizieren müssen, bevor Sie Informationen über Ihre Anforderung abrufen können.

5. In die folgenden Felder müssen Informationen eingegeben werden:
   - Bei **Anforderungs-ID** geben Sie die Anforderungs-ID ein, die nach Übergabe des Registrierungsformulars angezeigt wurde.
   - Bei **Identifikationsprüfungsantwort** geben Sie dieselbe Identifikationsprüfungsantwort ein, die Sie im Registrierungsformular angegeben haben.
6. Klicken Sie auf **Registrierungsstatus überprüfen**.

   Eine Nachricht zeigt den aktuellen Status Ihrer Anforderung an.
   - Wenn Ihre Anforderung noch anstehend ist, können Sie später hierher zurückkehren und den Status erneut überprüfen.
   - Wenn Ihre Anforderung genehmigt wurde, wird mit der Registrierungsart festgelegt, was als nächstes erfolgt.

     Browser-Zertifikat
     Das Browser-Zertifikat wird sofort auf Ihren Browser heruntergeladen.

     Server- oder Einheitenzertifikat
     Der Browser fordert Sie auf, ein Format auszuwählen und einen Pfad anzugeben. Anschließend wird das Server- oder Einheitenzertifikat zum Ziel des Pfads heruntergeladen.

     Vorabregistrierung von Zertifikaten
     Das Zertifikat wird erst dann übergeben, wenn die von Ihnen vorab registrierte Person es von der Trust Authority-Client-Anwendung anfordert.

     Stattdessen werden Informationen angezeigt, die der zukünftige Zertifikatsinhaber benötigt, um das Zertifikat anzufordern: eine Transaktions-ID, ein Kennwort und die URL der Registrierungsstelle (RA), die die Anforderung genehmigt hat.

     Anmerkung: Wenn Sie es wünschen, können Sie eine Vorabregistrierungsdatei zur Verfügung stellen. Diese kann beim Anfordern des Zertifikats zusammen mit dem Kennwort verwendet werden. Um eine Kopie abzurufen, klicken Sie auf **Vorabregistrierungsdatei sichern**, und geben Sie einen Pfad für die Datei an.

Verwaltung von Zertifikaten unter Verwendung eines Browsers

Auf der Registrierungs-Web-Seite können Sie ein Browser-Zertifikat, das Sie heruntergeladen haben, auch erneuern oder widerrufen. Gegebenenfalls können Sie das Zertifikat auch in den Wartestatus setzten, anstatt es permanent zu widerrufen. Dies gilt nicht für Zertifikate, für die Sie eine Vorabregistrierung vorgenommen haben.

Anmerkung: Wenn Sie eine Fehlernachricht erhalten, während Sie Zertifikate mit Hilfe von Microsoft Internet Explorer erneuern oder widerrufen, liegt dies unter Umständen daran, daß Sie keine SSL-Sitzung mit Client-Authentifizierung zum Web-Server herstellen können. Um dieses Problem zu lösen, wählen Sie im Browser **Extras → Internetoptionen** aus. Wählen Sie im Fenster für die Einstellungen der Internet-Optionen die Registerkarte **Erweitert** aus, und klicken Sie anschließend auf den Knopf **Standards wiederherstellen**. Dadurch wird SSL

Version 3.0 erneut aktiviert. Klicken Sie auf **OK**, und schließen Sie den Browser. Starten Sie Internet Explorer erneut, und versuchen Sie erneut, eine Verbindung zum Server herzustellen.

Ein Zertifikat in den Wartestatus setzen

Sie können Browser-Zertifikate, die Sie direkt über die Registrierungs-Web-Seite abgerufen haben, in den Wartestatus setzen.

Anmerkung: Wenn Sie Ihr Zertifikat heruntergeladen haben, als die Client-Anwendung aktiv war, müssen Sie diese Anwendung verwenden, um das Zertifikat in den Wartestatus zu setzen.

Um Ihr Zertifikat in den Wartestatus zu setzen, gehen Sie folgendermaßen vor:

1. Nehmen Sie Zugriff auf die Registrierungs-Web-Seite.
2. Wählen Sie über **Registrierungsart** die Option **Browser-Zertifikat** aus.
3. Wählen Sie über **Aktion**die Option **Widerrufen** aus.
4. Klicken Sie auf **OK**.

   Die Anzeige enthält Informationen, die Sie und das Zertifikat identifizieren.
5. Überprüfen Sie die Informationen, um sicherzustellen, daß dies auch tatsächlich das Zertifikat ist, das Sie in den Wartestatus setzen wollen.
6. Bei **Begründung** wählen Sie die Option **Zertifikat in den Wartestatus setzen** aus.
7. Bei **Datum, ab dem das Zertifikat nicht mehr gültig ist** geben Sie an, wann das Zertifikat in den Wartestatus gesetzt werden soll. Wählen Sie entweder das aktuelle Datum oder ein Datum in der Vergangenheit aus.
8. Klicken Sie auf **Zertifikat widerrufen**.

Anmerkung: Sofern das Zertifikat nicht abläuft, während es sich auf der Zertifikatswiderrufsliste (CRL) befindet, können Sie es später erneut aktivieren lassen.

Ein Zertifikat erneuern

Sie können Browser-Zertifikate erneuern, die Sie direkt über die Registrierungs-Web-Seite abgerufen haben.

Anmerkung: Wenn Sie Ihr Zertifikat heruntergeladen haben, als die Client-Anwendung aktiv war, müssen Sie diese Anwendung verwenden, um das Zertifikat zu erneuern.

Um ein Zertifikat zu erneuern, gehen Sie folgendermaßen vor:

1. Nehmen Sie Zugriff auf die Registrierungs-Web-Seite.
2. Wählen Sie über **Registrierungsart** die Option **Browser-Zertifikat** aus.
3. Wählen Sie über **Aktion** die Option **Erneuern** aus.
4. Klicken Sie auf **OK**.

   Ein Erneuerungsformular wird angezeigt.
5. Überprüfen Sie das Formular, um sicherzustellen, daß dies auch tatsächlich das Zertifikat ist, das Sie erneuern wollen.
6. Ändern Sie gegebenenfalls die Werte in den editierbaren Feldern. Im Abschnitt „Registrierungsformular auf der Web-Seite” auf Seite 33 werden die Felder beschrieben.

E-Mail-Adresse
Um **E-Mail-Benachrichtigung** auswählen zu können, müssen Sie Ihre E-Mail-Adresse angeben.

E-Mail-Benachrichtigung
Wählen Sie dieses Feld aus, wenn Sie per E-Mail vom Ergebnis Ihrer Anforderung informiert werden wollen.

Identifikationsprüfungsfrage
Sie können die Frage ändern, die Ihnen gestellt wird, wenn Sie den Status Ihrer Anforderung überprüfen.

Identifikationsprüfungsantwort
Stellen Sie sicher, daß Sie die von Ihnen angegebene **Identifikationsprüfungsantwort** (von Groß-/Kleinschreibung abhängig) nicht vergessen. Sie benötigen die Antwort später, um den Status der Registrierungsanforderung überprüfen zu können.

Für Internet Explorer

- Befolgen Sie die Anweisungen auf dem Formular, wenn Sie den Provider für Ihren Verschlüsselungsservice wechseln wollen.
- Entscheiden Sie, ob ein neuer Schlüsselsatz erstellt oder der vorhandene erneut verwendet werden soll. Soll ein neuer Schlüsselsatz erstellt werden, haben Sie die Möglichkeit, ihn selbst zu benennen.
- Wählen Sie **Zusätzliche Sicherheitsoptionen** aus, um gegebenenfalls weitere Sicherheitsmaßnahmen von Microsoft Internet Explorer anzufordern.

7. Klicken Sie auf **Zertifikat erneuern**.
8. Merken Sie sich Ihre Anforderungs-ID, wenn diese angezeigt wird, damit Sie später den Status der Anforderung überprüfen können. Im Abschnitt „Den Registrierungsstatus überprüfen" auf Seite 10 wird beschrieben, wie Sie den Status Ihrer Anforderung überprüfen können.

Ein Zertifikat widerrufen

Sie können Browser-Zertifikate widerrufen, die Sie direkt über die Registrierungs-Web-Seite abgerufen haben.

Anmerkung: Wenn Sie Ihr Zertifikat heruntergeladen haben, als die Client-Anwendung aktiv war, müssen Sie diese Anwendung verwenden, um das Zertifikat zu widerrufen.

Um ein Zertifikat zu widerrufen, gehen Sie folgendermaßen vor:

1. Nehmen Sie Zugriff auf die Registrierungs-Web-Seite.
2. Wählen Sie über **Registrierungsart** die Option **Browser-Zertifikat** aus.
3. Wählen Sie über **Aktion** die Option **Widerrufen** aus.
4. Klicken Sie auf **OK**.

   Es werden Informationen zur Identifizierung des Zertifikats angezeigt.
5. Überprüfen Sie die Informationen, um sicherzustellen, daß dies auch das Zertifikat ist, das Sie widerrufen wollen.
6. Bei **Begründung** wählen Sie einen Grund aus, warum Sie das Zertifikat widerrufen wollen. Im Abschnitt „Begründung für den Widerruf von Zertifikaten" auf Seite 37 werden die zulässigen Gründe beschrieben.
7. Bei **Datum, ab dem das Zertifikat nicht mehr gültig ist** geben Sie an, wann das Zertifikat widerrufen werden soll. Wählen Sie entweder das aktuelle

Datum oder ein Datum in der Vergangenheit aus. Wenn die Begründung mit einem Datum zusammenhängt, verwenden Sie dieses Datum. Beispiel: Wenn Sie glauben, daß Ihr Schlüssel beschädigt wurde, wählen Sie das Datum aus, an dem dies Ihrer Meinung nach passiert ist.

8. Klicken Sie auf **Zertifikat widerrufen**.

Aktive Anforderungen abbrechen

Wenn Sie eine Anforderung übergeben, um ein Zertifikat zu erneuern, zu widerrufen oder in den Wartestatus zu setzen, und versuchen, diese Anforderung nach der Übergabe abzubrechen, gibt der Browser eine Fehlernachricht mit dem Inhalt "Dokument enthält keine Daten" zurück. Des weiteren kann der Browser die Registrierungs-Web-Seite nicht erneut anzeigen.

Dieser Fehler kann auftreten, wenn der Browser die Anforderung an den RA-Server weiterleitet, bevor er Sie zur Vorlage eines Zertifikats für die Authentifizierung auffordert. Wenn das Zertifikat nicht zusammen mit der Anforderung übergeben wird, wird ein Fehler zurückgegeben. Dies stellt die normale Browser-Funktionsweise dar. In dieser Situation kann der Browser nicht identifizieren, welches Zertifikat abgebrochen werden soll, nachdem der Knopf **Abbrechen** angeklickt wurde.

Mit mehreren Zertifikaten arbeiten

Wenn Sie eine Anforderung übergeben, um ein Zertifikat zu erneuern, zu widerrufen oder in den Wartestatus zu setzen, und anschließend die Registrierungs-Web-Seite erneut aufrufen, um mit einem anderen Zertifikat zu arbeiten, so ist dies erst dann möglich, wenn Sie den Browser beendet und erneut gestartet haben. Dies stellt die normale Browser-Funktionsweise dar. Sie müssen das aktuelle Zertifikat zunächst aus dem Browser-Cache löschen, bevor Sie versuchen, ein weiteres Zertifikat zu bearbeiten.

Ebenso kann ein Zertifikat, nachdem es heruntergeladen wurde, nicht in derselben Browser-Sitzung erneuert oder widerrufen werden. Sie müssen den Browser beenden, bevor Sie versuchen, ein neu installiertes Zertifikat zu bearbeiten.

Client-Anwendung installieren

Der Prozeß zur Installation von Trust Authority Client besteht aus zwei Teilen. Beim Installieren der Server-Software muß ein Systemadministrator Trust Authority Client auswählen, um das Installationsabbild für die Anwendung zu installieren. Der Administrator muß das Abbild anschließend verteilen oder es auf dem Netz zur Verfügung stellen, damit Sie das Installationsprogramm über Ihre Datenstation ausführen können.

Verwenden Sie die folgende Prozedur, um das Installationsprogramm der Client-Anwendung (TACInst.exe) auszuführen.

1. Stellen Sie sicher, daß Ihre Datenstation die im Abschnitt „Systemvoraussetzungen für die Client-Anwendung" auf Seite 38 aufgeführten Anforderungen erfüllt.
2. Befolgen Sie die Anweisungen Ihres Unternehmens, um das Client-Installationsabbild zu kopieren, herunterladen oder darauf zuzugreifen.
3. Fahren Sie alle aktiven Programme herunter.
4. Wählen Sie **Starten → Ausführen** aus, klicken Sie auf **Durchsuchen**, um die Datei 'TACInst.exe' zu suchen, und klicken Sie dann auf **OK**, um das Programm auszuführen.

5. Lesen Sie die Anweisungen im Eingangsfenster, und klicken Sie auf **Weiter**.
6. Klicken Sie im Fenster für die Suche nach der Zieladresse auf **Weiter**, wenn Sie die Software unter dem Standardverzeichnis (c:\Program Files\IBM\Trust Authority) installieren wollen. Ansonsten klicken Sie auf **Durchsuchen**, um einen anderen Zielordner auszuwählen oder einzugeben. Klicken Sie anschließend auf **Weiter**.

   Anmerkung: Wenn Sie bereits zuvor eine Trust Authority-Komponente auf dieser Datenstation installiert haben, wird die Software automatisch im Unterverzeichnis 'TAClient' an derselben Position installiert. Sie werden nicht aufgefordert, eine Zielposition anzugeben.
7. Klicken Sie im Fenster für die Auswahl des Programmordners auf **Weiter**, wenn Sie den Standardprogrammordner (IBM SecureWay Trust Authority) verwenden wollen. Ansonsten wählen Sie den Namen des gewünschten Ordners aus oder geben diesen ein und klicken anschließend auf **Weiter**.
8. Geben Sie im Fenster zum Öffnen der Smart Card ein Kennwort für Ihre virtuelle Smart Card ein. Geben Sie denselben Namen zur Bestätigung erneut ein, und klicken Sie anschließend auf **Weiter**. Sie müssen dieses Kennwort, das höchstens acht Zeichen enthalten darf, beim Starten der Client-Anwendung eingeben.

   An dieser Stelle kopiert das System die entsprechenden Dateien in die angeforderte Installationsposition und führt entsprechende Programme aus, um die Installation der Client-Anwendung abzuschließen.
9. Geben Sie im Fenster für den Abschluß der Funktion Setup an, ob Sie Windows jetzt oder zu einem späteren Zeitpunkt erneut starten wollen, und klicken Sie anschließend auf **Fertig**. Wenn Sie das System zu einem späteren Zeitpunkt erneut starten wollen, müssen Sie dies vor Verwendung der Client-Anwendung tun.

   Nach Abschluß der Installation befindet sich **Trust Authority Client** im Menü **Start** unter **Programme → IBM SecureWay Trust Authority**.

Hinweise zur Verwendung:

- Wenn Sie eine Fehlernachricht erhalten, in der Ihnen mitgeteilt wird, daß CSSM32.dll im angegebenen Pfad nicht gefunden werden kann, führen Sie das Installationsprogramm für die Client-Anwendung erneut aus. Auf diese Weise wird der Fehler normalerweise behoben.
- Wenn Sun Java Runtime Environment (JRE) oder Java Development Kit (JDK) bereits auf der Maschine installiert wurde, auf der Sie den Client installieren möchten, und Sie eine Fehlernachricht erhalten, in der Ihnen mitgeteilt wird, daß JRE nicht gefunden werden kann, müssen Sie die Variable PATH für diese Maschine aktualisieren, um sicherzustellen, daß sie den Installationspfad des Programms 'jre.exe' enthält.

Physische Smart Cards aktivieren

Nach der Installation der Trust Authority Client-Anwendung müssen Sie folgende Schritte ausführen, um Zertifikate, die sich auf einer physischen Smart Card befinden, aufrufen und dort speichern zu können.

1. Befolgen Sie die mit Ihrer Smart Card gelieferte Prozedur, um die Karte und die Software zu installieren. Sie können beispielsweise eines der folgenden Produkte installieren:
   - IBM Smart Card Security Kit for Desktop Systems (für die Serienversion)
   - IBM Smart Card Security Kit for Notebook Computers (für die PCMCIA-Version)

2. Bearbeiten Sie die Datei 'TAClient.ini'. Der Standardpfad für diese Datei lautet: c:\Program Files\IBM\Trust Authority\TAClient.
3. Ändern Sie den Abschnitt [KeyStore] folgendermaßen:

```
Ändern:
  [KeyStore]
  CurKeyStore=VSC
in:
  [KeyStore]
  CurKeyStore=SmartCard
```

4. Ändern Sie den Abschnitt [SmartCard] folgendermaßen:

```
Ändern
  [SmartCard]
  Model=PKCS11_STORAGE_MODEL
  Guid=EA8A7C01-13BC-11d3-B150-002035C00173
  LibraryName=
in:
  [SmartCard]
  Model=PKCS11_STORAGE_MODEL
  Guid=EA8A7C01-13BC-11d3-B150-002035C00173
  LibraryName=c:\winnt\system32\W32pk2ig.dll
```

   Anmerkung: `LibraryName` steht in diesem Beispiel für den Standardpfad von W32pk2ig.dll für ein Windows NT-System, das auf dem Laufwerk C: installiert ist. Die Position dieser Datei kann auf Ihrem System unterschiedlich sein.

5. Geben Sie die folgenden Befehle ein, um das Programm 'initsc' auszuführen. Sie werden nicht zur Eingabe von Kennwörtern aufgefordert (die Kennwörter bleiben dieselben, die Sie beim Installieren der physischen Smart Card festgelegt haben).

```
cd "c:\Program Files\IBM\Trust Authority\bin"
initsc -e ee -i c:\Program Files\IBM\Trust Authority\TAClient\TAClient.ini
```

Wenn Sie die Smart Card mit der Client-Anwendung verwenden, denken Sie daran, daß die Karte ein 512–Bit-Schlüsselpaar, ein 1024–Bit-Schlüsselpaar und die entsprechenden Zertifikate enthalten kann. Wenn Sie versuchen, ein zweites 512–Bit-Schlüsselpaar oder ein zweites 1024–Bit-Schlüsselpaar zu generieren, erhalten Sie eine Speicherfehlernachricht.

Die Client-Anwendung aufrufen

Mit der Client-Anwendung können Sie ein Zertifikat anfordern und dann auf Ihrer virtuellen oder physischen Smart Card speichern, nachdem Sie von jemandem vorab registriert wurden. Sie können die Client-Anwendung auch dazu verwenden, die Zertifikate auf Ihren Smart Cards und die Smart Cards selber zu verwalten. Alle diese Zertifikate sind für den Zugriff auf PKIX-kompatible Anwendungen geeignet.

Um die Client-Anwendung aufzurufen, gehen Sie folgendermaßen vor:

1. Wenn Sie Ihre physische Smart Card verwenden wollen, legen Sie diese ein.
2. Wählen Sie in der Task-Leiste von Windows nacheinander **Start → Programme → IBM SecureWay Trust Authority → Trust Authority Client** aus.
3. Klicken Sie in der Eingangsanzeige auf **OK**.

   Der Dialog 'Smart Card öffnen' wird angezeigt. Er enthält eine Liste Ihrer Smart Cards, die für die Client-Anwendung definiert sind. Auf Seite 44 wird dieser Dialog beschrieben.
4. Wählen Sie über **Smart Card** die Smart Card aus, die Sie öffnen wollen.

5. Bei **Kennwort** geben Sie Ihr Kennwort für die ausgewählte Smart Card ein.
6. Klicken Sie auf **OK**.

   Das Fenster 'Smart Card' wird angezeigt. Auf Seite 39 wird dieses Fenster beschrieben.

   Anmerkung: Liegen Zertifikate vor, die demnächst ablaufen, zeigt die Client-Anwendung Ihnen diese Zertifikate an, damit Sie entscheiden können, ob Sie die Zertifikate erneuern wollen oder nicht. Im Abschnitt „Demnächst ablaufende Zertifikate erneuern" auf Seite 20 wird beschrieben, was in diesem Fall zu tun ist.

Über den Client registrieren

Bevor Sie ein Zertifikat über die Client-Anwendung anfordern können, müssen Sie sich auf der Registrierungs-Web-Seite von Trust Authority vorab registrieren. Ihr Registrator, ein Benutzer mit Berechtigung zur Verwaltung von Registrierungsanforderungen, wird Sie möglicherweise vorab registrieren.

Nachdem Sie die Vorabregistrierungsinformationen erhalten haben, verwenden Sie die Client-Anwendung, um ein Zertifikat anzufordern. Die Art der von Ihnen empfangenen Vorabregistrierungsinformationen legt fest, welche Client-Menüoption zu wählen ist:

- Eine Vorabregistrierungsdatei
- Eine Transaktions-ID

Registrierung unter Verwendung einer Vorabregistrierungsdatei

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Öffnen Sie das Menü **Zertifikat**, und klicken Sie nacheinander auf **Neu** → **Verwendung einer Vorabregistrierungsdatei**.

   Der Dialog 'Neues Zertifikat unter Verwendung einer Vorabregistrierungsdatei' wird angezeigt. Auf Seite 42 wird dieser Dialog beschrieben.
2. Füllen Sie die Felder in diesem Dialog aus, und klicken Sie auf **Weiter**.

   Was als nächstes im Dialog angezeigt wird, hängt von den Wünschen Ihres Unternehmens ab. Es gibt folgende Möglichkeiten:

   - Attribute und ihre Werte, die Ihre Zertifikatsanforderung beschreiben.
   - Felder im unteren Bereich der Anzeige, in denen Sie einige Attributwerte durch Überschreiben ändern können.
3. Nehmen Sie gegebenenfalls die erforderlichen Änderungen vor.
4. Klicken Sie auf **Weiter**, um die Anforderung zu übergeben.
5. Klicken Sie im Bestätigungsfenster auf **Fertigstellen**.

Nachdem die Registrierungsstelle Ihre Anforderung genehmigt hat, wird Ihr Zertifikat automatisch auf der Smart Card gespeichert, die geöffnet ist.

Registrierung unter Verwendung einer Transaktions-ID

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Öffnen Sie das Menü **Zertifikat**, und klicken Sie nacheinander auf **Neu** → **Verwendung einer Transaktions-ID**.

   Der Dialog 'Neues Zertifikat unter Verwendung einer Transaktions-ID' wird angezeigt. Auf Seite 43 wird dieser Dialog beschrieben.

2. Füllen Sie die Felder aus.
3. Klicken Sie auf **Weiter**, um die Anforderung zu übergeben.
4. Klicken Sie im Bestätigungsfenster auf **Fertigstellen**.

Nachdem die Registrierungsstelle Ihre Anforderung genehmigt hat, wird Ihr Zertifikat automatisch auf der Smart Card gespeichert, die geöffnet ist.

Verwaltung von Zertifikaten unter Verwendung des Client

Mit der Client-Anwendung können Sie alle eigenen Zertifikate verwalten, die sich auf der Smart Card befinden, die geöffnet ist. Wenn Sie mit einem Zertifikat arbeiten wollen, das sich auf einer anderen Smart Card befindet, oder wenn Sie ein Zertifikat auf eine andere Smart Card herunterladen wollen, müssen Sie die Client-Anwendung schließen und anschließend mit der Smart Card, die Sie verwenden wollen, erneut starten.

Ein Zertifikat oder eine anstehende Anforderung löschen

Anmerkung: Diese Aktion kann nur schwer widerrufen werden, und unter Umständen ist dies überhaupt nicht möglich. Bevor Sie ein Zertifikat oder eine Anforderung, die Sie während der Verwaltung Ihrer Zertifikate ausgegeben haben, löschen, nehmen Sie sich die Zeit, die entsprechende Beschreibung noch einmal zu überprüfen. Bestätigen Sie anschließend, daß Sie das Zertifikat bzw. die Anforderung, die sich auf das Zertifikat bezieht, tatsächlich löschen wollen.

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Wählen Sie das Zertifikat oder die anstehende Anforderung aus, das bzw. die Sie löschen wollen.
2. Öffnen Sie das Menü **Zertifikat**, und klicken Sie nacheinander auf **Löschen →Zertifikat löschen**.
3. Der Dialog 'Zertifikat löschen' wird angezeigt. Auf Seite 41 wird dieser Dialog beschrieben.
4. Überprüfen Sie im Dialog die Beschreibung des Zertifikats oder der anstehenden Anforderung. Auf Seite 43 werden die angezeigten Details beschrieben.
5. Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen, oder klicken Sie auf **Abbrechen**, wenn Sie Ihre Meinung geändert haben.

Ein Zertifikat von einer Smart Card in eine Datei exportieren

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Wählen Sie das Zertifikat aus, das Sie von der geöffneten Smart Card exportieren wollen.
2. Öffnen Sie das Menü **Zertifikat**, und klicken Sie auf **Exportieren**.
3. Der Dialog 'Zertifikat exportieren' wird angezeigt. Auf Seite 42 wird dieser Dialog beschrieben.
4. Wählen Sie die Verschlüsselungsart aus, die zur Verschlüsselung des Zertifikats verwendet werden soll.
5. Geben Sie die Position für die Erstellung einer Datei an, in der das Zertifikat gespeichert werden soll. Geben Sie dazu entweder den Pfad und den Dateinamen ein, oder klicken Sie auf **Anzeigen**, um einen Pfad auszuwählen und dann einen Dateinamen einzugeben.

6. Geben Sie ein Kennwort zum Schutz der Datei ein, und bestätigen Sie es durch nochmalige Eingabe. Für das Kennwort können Sie 8 bis 32 alphanumerische Zeichen verwenden.
7. Klicken Sie auf **OK**, oder klicken Sie auf **Abbrechen**, wenn Sie Ihre Meinung geändert haben.

Ein Zertifikat aus einer Datei auf eine Smart Card importieren

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Wählen Sie das Zertifikat aus, das Sie auf die geöffnete Smart Card importieren wollen.
2. Öffnen Sie das Menü **Zertifikat**, und klicken Sie auf **Importieren**.
3. Der Dialog 'Zertifikat importieren' wird angezeigt. Auf Seite 42 wird dieser Dialog beschrieben.
4. Geben Sie die aktuelle Position der Datei an, an der sich das Zertifikat befindet. Geben Sie dazu entweder den Pfad und den Dateinamen ein, oder klicken Sie auf **Anzeigen**, um beides auszuwählen.
5. Geben Sie das Kennwort ein, das Sie beim Exportieren des Zertifikats in die Datei erstellt haben.
6. Geben Sie einen aussagekräftigen Namen ein, um das Zertifikat auf der Smart Card erkennen zu können.
7. Klicken Sie auf **OK**, oder klicken Sie auf **Abbrechen**, wenn Sie Ihre Meinung geändert haben.

Ein Zertifikat auf eine andere Smart Card verschieben

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Wählen Sie das Zertifikat aus, das Sie von der geöffneten Smart Card auf eine andere Smart Card verschieben wollen.
2. Führen Sie die Schritte zum Exportieren dieses Zertifikats in eine Datei aus. Im Abschnitt „Ein Zertifikat von einer Smart Card in eine Datei exportieren" auf Seite 18 werden diese Schritte beschrieben.
3. Verlassen Sie die Client-Anwendung.
4. Wenn Sie das Zertifikat auf eine physische Smart Card verschieben wollen, laden Sie diese Smart Card.
5. Starten Sie die Client-Anwendung erneut, und öffnen Sie diesmal die zuvor geladene Smart Card. Im Abschnitt „Eine andere Smart Card öffnen" auf Seite 23 wird beschrieben, wie dabei vorzugehen ist.
6. Führen Sie die Schritte zum Importieren des Zertifikats aus der Datei auf die geöffnete Smart Card aus. Im Abschnitt „Ein Zertifikat aus einer Datei auf eine Smart Card importieren" werden diese Schritte beschrieben.

Ein Zertifikat zum Anzeigen von Details öffnen

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Wählen Sie das Zertifikat aus, für das Sie Details anzeigen wollen.
2. Öffnen Sie das Menü **Zertifikat**, und klicken Sie auf **Öffnen**.
3. Der Dialog 'Zertifikat öffnen' wird angezeigt. Auf Seite 43 wird dieser Dialog beschrieben.
4. Überprüfen Sie im Dialog die Beschreibung des Zertifikats.
5. Klicken Sie auf **OK**, wenn Sie mit der Überprüfung fertig sind.

Ein Zertifikat in den Wartestatus setzen

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Wählen Sie das Zertifikat aus, das Sie in den Wartestatus setzen wollen.
2. Öffnen Sie das Menü **Zertifikat**, und klicken Sie auf **Widerrufen**.
3. Der Dialog 'Zertifikat widerrufen' wird angezeigt. Auf Seite 45 wird dieser Dialog beschrieben.
4. Überprüfen Sie im Dialog die Beschreibung des Zertifikats. Die Beschreibung enthält die Seriennummer und den Aussteller. Auf Seite 43 werden die angezeigten Details beschrieben.
5. Bei **Begründung** wählen Sie die Option **Zertifikat in den Wartestatus setzen** aus.
6. Wählen Sie über die **URL der RA** (sofern das Feld nicht bereits ausgefüllt ist) die URL der Registrierungsstelle aus, die Ihre ursprüngliche Zertifikatsanforderung genehmigt hat, oder geben Sie die entsprechende URL ein.
7. Klicken Sie auf **OK**, oder klicken Sie auf **Abbrechen**, wenn Sie Ihre Meinung geändert haben.

Anmerkung: Sofern das Zertifikat nicht abläuft, während es sich auf der Zertifikatswiderrufsliste (CRL) befindet, können Sie Ihren Registrator bitten, es später erneut zu aktivieren.

Ein Zertifikat erneuern

Wenn Sie ein Zertifikat erneuern, dann hat das neue Zertifikat dieselbe Gültigkeitsdauer wie das alte. Sie können entweder das Schlüsselpaar des alten Zertifikats verwenden oder ein neues Schlüsselpaar generieren.

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Wählen Sie das Zertifikat aus, das Sie erneuern wollen.
2. Öffnen Sie das Menü **Zertifikat**, und klicken Sie auf **Erneuern**.
3. Der Dialog 'Zertifikat erneuern' wird angezeigt. Auf Seite 45 wird dieser Dialog beschrieben.
4. Überprüfen Sie im Dialog die Beschreibung des Zertifikats. Die Beschreibung enthält die Seriennummer und den Aussteller. Auf Seite 43 werden die angezeigten Details beschrieben.
5. Wählen Sie über die **URL der RA** (sofern das Feld nicht bereits ausgefüllt ist) die URL der Registrierungsstelle aus, die Ihre ursprüngliche Zertifikatsanforderung genehmigt hat, oder geben Sie die entsprechende URL ein.
6. Wenn Sie das alte Schlüsselpaar nicht verwenden wollen, wählen Sie aus der Liste mit den Alternativen einen neuen Algorithmus und eine neue Schlüsselgröße aus. Alle aufgelisteten Algorithmen und Größen sind für Ihre Maschine geeignet.
7. Klicken Sie auf **OK**, oder klicken Sie auf **Abbrechen**, wenn Sie Ihre Meinung geändert haben.

Demnächst ablaufende Zertifikate erneuern

Ihr Unternehmen hat festgelegt, zu welchem Zeitpunkt Sie eine Warnung erhalten sollen, wenn ein Zertifikat demnächst abläuft. Der Standardwert beträgt 30 Tage vor Ablauf.

Wenn ein Zertifikat in ihrer geöffneten Smart Card demnächst abläuft, wird es im Dialog 'Zertifikatserneuerung' angezeigt, wenn Sie die Client-Anwendung starten. Die betreffenden Zertifikate werden in einer Tabelle aufgelistet, die auch über Spalten mit einer Zusammenfassung der Beschreibungen verfügt. Auf Seite 43 werden die angezeigten Details beschrieben.

1. Überprüfen Sie die Zertifikate. Gegebenenfalls können Sie die Anzeige anpassen.
   - Vergrößern Sie das Fenster, wenn Sie in der Tabelle mehr Zeilen anzeigen wollen.
   - Ändern Sie die Größe einer Spalte, um mehr Daten anzuzeigen.
2. Wählen Sie die Zertifikate aus, die Sie erneuern wollen, und klicken Sie auf **OK**.

   Der Dialog 'Zertifikat erneuern' wird für jedes ausgewählte Zertifikat angezeigt. Auf Seite 41 wird dieser Dialog beschrieben.
3. Füllen Sie für jedes Zertifikat die Felder des Dialogs aus, und klicken Sie auf **OK**.

Anmerkung: Wenn Sie keine Zertifikate auswählen, können Sie den Dialog einfach schließen, indem Sie auf **OK** klicken.

Ein Zertifikat widerrufen

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Wählen Sie das Zertifikat aus, das Sie widerrufen wollen.
2. Öffnen Sie das Menü **Zertifikat**, und klicken Sie auf **Widerrufen**.
3. Der Dialog 'Zertifikat widerrufen' wird angezeigt. Auf Seite 45 wird dieser Dialog beschrieben.
4. Überprüfen Sie im Dialog die Beschreibung des Zertifikats. Auf Seite 43 werden die angezeigten Details beschrieben.
5. Bei **Begründung für den Widerruf**, wählen Sie einen Grund aus, warum Sie das Zertifikat widerrufen wollen. Im Abschnitt „Begründung für den Widerruf von Zertifikaten" auf Seite 37 werden die zulässigen Gründe aufgelistet.
6. Wählen Sie über die **URL der RA** (sofern das Feld nicht bereits ausgefüllt ist) die URL der Registrierungsstelle aus, die Ihre ursprüngliche Zertifikatsanforderung genehmigt hat, oder geben Sie die entsprechende URL ein.

   Anmerkung: Sie haben diese URL im Anschluß an Ihre Vorabregistrierung erhalten und haben sie verwendet, um Ihr Zertifikat anzufordern.
7. Klicken Sie auf **OK**, oder klicken Sie auf **Abbrechen**, wenn Sie Ihre Meinung geändert haben.

Dateien unterzeichnen

Sie können ein Zertifikat verwenden, um eine Datei zu unterzeichnen. Wenn Sie eine Datei mit einer digitalen Unterschrift unterzeichnen, kann jeder, der die Datei öffnet, erkennen, ob der Inhalt der Datei seit der Unterzeichnung geändert wurde. Es ist zu beachten, daß der Inhalt der Datei mit der digitalen Unterschrift nicht verschlüsselt wird.

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Wählen Sie das Zertifikat aus, das Sie zur Unterzeichnung der Datei verwenden wollen.

2. Öffnen Sie das Menü **Zertifikat**, und klicken Sie auf **Unterzeichnen**. Der Dialog zum Unterzeichnen einer Datei wird angezeigt.
3. Geben Sie bei **Eingabedateiname** den Pfad und den Namen der Datei an, die Sie unterzeichnen wollen. Geben Sie dazu entweder den Pfad und den Dateinamen ein, oder klicken Sie auf **Durchsuchen**, um den Pfad der Datei auszuwählen.
4. Geben Sie bei **Ausgabedateiname** einen Pfad und einen Namen für die unterzeichnete Datei an. Klicken Sie auf **Durchsuchen**, um den Pfad und den Dateinamen auszuwählen, anstatt diese Angaben manuell einzugeben.
5. Wählen Sie bei **Unterschriftsalgorithmus** den Algorithmus aus, den Sie verwenden wollen, um die Datei digital zu unterzeichnen. Auf der Seite 46 werden die verfügbaren Auswahlmöglichkeiten beschrieben.
6. Wenn Sie die Datei vor dem Unterzeichnen anzeigen wollen, klicken Sie auf **Anzeigen**. Mit dieser Aktion wird die Anwendung aufgerufen, die dem Dateityp der unterzeichneten Datei zugeordnet ist. Wenn Sie beispielsweise eine HTML-Datei unterzeichnen, ruft die Anwendung Ihren Standard-Browser auf, um die Datei anzuzeigen.
7. Klicken Sie auf **OK**, um die Datei zu unterzeichnen, oder klicken Sie auf **Abbrechen**, wenn Sie Ihre Meinung geändert haben.

Mit einer Zertifikatliste arbeiten

Im Fenster 'Smart Card' zeigen die Registerkarten die Zertifikate nach Kategorien an:

- Um eine Liste Ihrer eigenen Zertifikate anzuzeigen, klicken Sie auf die Registerkarte **Meine Zertifikate**.
- Um die Liste der anderen Zertifikate auf derselben Smart Card anzuzeigen, klicken Sie auf die Registerkarte **Andere Zertifikate**. (Sofern Sie die Smart Card nicht mit jemandem gemeinsam benutzen, sind keine anderen Zertifikate vorhanden.)

In einer Tabelle werden die Basisinformationen zu jedem Zertifikat angezeigt.

- Blättern Sie gegebenenfalls durch die Spalten, oder ändern Sie deren Größe, um alle Informationen anzuzeigen.
- Wählen Sie gegebenenfalls ein Zertifikat aus.

Zwischen Registerkarten wechseln

Im Fenster 'Smart Card' ist die gerade angezeigte Registerkarte heller dargestellt als die andere.

Um von einer Registerkarte zur anderen zu wechseln, klicken Sie einfach die jeweils andere Registerkarte an.

Mehr Zeilen in einer Tabelle anzeigen

Um mehr Zeilen in einer Tabelle eines Fensters der Client-Anwendung oder des Dialogs 'Zertifikatserneuerung' anzuzeigen, führen Sie eine der folgenden Aktionen aus:

- Blättern Sie durch die Tabelle, um weitere Zeilen zu sehen.
- Vergrößern Sie das Fenster oder den Dialog, um einen größeren Ausschnitt der Tabelle anzuzeigen.

Die Größe einer Tabellenspalte ändern

Um die Größe einer Tabellenspalte zu ändern, gehen Sie folgendermaßen vor:

1. Verschieben Sie den Cursor auf die Begrenzung der Spalte, deren Größe Sie ändern wollen.
2. Klicken Sie mit der Maustaste, halten Sie die Taste gedrückt, und ziehen Sie die Maus nach rechts oder links, um die Spaltenbreite zu ändern.
3. Lassen Sie die Maustaste los, sobald die Spalte die gewünschte Breite hat.

Verwaltung von Smart Cards unter Verwendung des Client

In diesem Abschnitt werden die allgemeinen Tasks im Zusammenhang mit der Verwendung und Verwaltung von Smart Cards erläutert.

Eine andere Smart Card öffnen

Sie können eine Smart Card immer dann öffnen, wenn Sie die Client-Anwendung aufrufen. Die Standard-Smart Card ist eine virtuelle Smart Card. Wenn Sie auch über eine physische Smart Card verfügen, kann Ihr Administrator diese Karte für die Client-Anwendung definieren.

Um mit einer anderen Smart Card zu arbeiten, als derjenigen, die Sie zum jeweiligen Zeitpunkt angegeben haben, gehen Sie folgendermaßen vor:

1. Verlassen Sie die Client-Anwendung.
2. Wenn Sie Ihre physische Smart Card verwenden wollen, legen Sie diese ein.
3. Starten Sie die Client-Anwendung erneut.
4. Klicken Sie in der Eingangsanzeige auf **OK**.

   Der Dialog 'Smart Card öffnen' wird angezeigt. Er enthält eine Liste Ihrer Smart Cards, die für die Client-Anwendung definiert sind. Auf Seite 44 wird dieser Dialog beschrieben.
5. Wählen Sie über **Smart Card** die Smart Card aus, die Sie öffnen wollen.
6. Bei **Kennwort** geben Sie Ihr Kennwort für die ausgewählte Smart Card ein.
7. Klicken Sie auf **OK**.

   Das Fenster 'Smart Card' wird angezeigt.

Ein Smart Card-Kennwort ändern

Anmerkung: Über diesen Dialog können Sie lediglich das Kennwort einer geöffneten virtuellen Smart Card ändern. Wenn Sie eine physische Smart Card haben, lesen Sie die mit dieser Karte gelieferte Dokumentation. Sie enthält Anweisungen für die Kennwortänderung.

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Öffnen Sie das Menü **Smart Card**, und klicken Sie **Kennwort ändern** an.

   Der Dialog 'Kennwort ändern' wird angezeigt. Auf Seite 41 wird dieser Dialog beschrieben.
2. Geben Sie das aktuelle Kennwort für Ihre virtuelle Smart Card ein.
3. Geben Sie Ihr neues Kennwort ein, und bestätigen Sie es durch nochmalige Eingabe. Für das Kennwort können Sie 8 bis 32 alphanumerische Zeichen verwenden. Achten Sie darauf, daß Sie sich das Kennwort leicht merken können.

Anmerkung: Die Kennwörter werden bei der Eingabe nicht angezeigt.

4. Klicken Sie auf **OK**, oder klicken Sie auf **Abbrechen**, wenn Sie Ihre Meinung geändert haben.

Smart Card-Eigenschaften anzeigen

Führen Sie im Fenster 'Smart Card' die folgenden Aktionen aus:

1. Öffnen Sie das Menü **Smart Card**, und klicken Sie auf **Eigenschaften anzeigen**.

   Der Dialog 'Smart Card-Eigenschaften' wird angezeigt. Auf Seite 46 wird dieser Dialog beschrieben.
2. Überprüfen Sie im Dialog die Beschreibung der Smart Card.
3. Klicken Sie auf **OK**, wenn Sie mit der Überprüfung fertig sind.

Client-Anwendung verlassen

Um die Client-Anwendung zu verlassen, gehen Sie folgendermaßen vor:

1. Wenn ein Dialog geöffnet ist, beenden Sie den Dialog, und klicken Sie auf **OK**, oder klicken Sie auf **Abbrechen**.
2. Öffnen Sie im Fenster 'Smart Card' das Menü **Smart Card**, und klicken Sie auf **Beenden**.

Client-Anwendung deinstallieren

Verwenden Sie folgende Prozedur, wenn Sie die Trust Authority Client-Anwendung von Ihrem System entfernen müssen.

1. Wählen Sie **Start → Einstellungen → Systemsteuerung** aus.
2. Klicken Sie doppelt auf **Software**.
3. Wählen Sie den Programmordner **IBM SecureWay Trust Authority Client** aus, und klicken Sie auf **Hinzufügen/Entfernen**.
4. Wenn Sie aufgefordert werden zu bestätigen, daß Sie das Programm löschen wollen, klicken Sie auf **Ja**.
5. Wenn Sie eine Nachricht erhalten, in der Ihnen mitgeteilt wird, daß bestimmte Ordner nicht gelöscht werden, klicken Sie auf **Details**. Sie müssen alle Ordner, die im Detailfenster aufgelistet sind, manuell löschen, um die Client-Anwendung vollständig von Ihrem System zu löschen.

Anmerkung: Wenn Sie nicht in der Lage sind, die Client-Anwendung zu deinstallieren, versuchen Sie, für das System einen Warmstart durchzuführen. Dadurch werden normalerweise gemeinsam benutzte Dateien freigegeben, so daß Sie diese löschen können. Wenn Sie das Menü **Software** von Windows weiterhin nicht verwenden können, um die Anwendung zu deinstallieren, müssen Sie die Windows-Registrierung möglicherweise manuell bearbeiten, um die Client-Einträge zu entfernen.

Kapitel 4. Erläuterungen

Die folgenden Abschnitte definieren und beschreiben Konzepte, die mit Zertifikaten, der Registrierung, der Zertifizierung und dem Zugriff auf gesicherte Ressourcen im Zusammenhang stehen.

Registrierung

Registrierung bedeutet die Beantragung eines Zertifikats. Trust Authority bietet mehrere Registrierungsmethoden; die Regeln Ihres Unternehmens legen fest, welche Methoden; zur Verfügung stehen. Sie können über Ihren Web-Browser auf die Registrierungsformulare zugreifen, wenn Sie ein Zertifikat anfordern müssen. Auf der Registrierungs-Web-Seite können Sie eine Verbindung zu einem Registrierungsformular herstellen, dieses ausfüllen und anschließend übergeben. Sie können die folgenden Aktionen ausführen:

- Ein CA-Zertifikat anfordern, um sich auf Ihre Registrierungs-Tasks vorzubereiten.
- Ein Browser-Zertifikat für sich selbst anfordern.
- Ein Zertifikat für eine(n) bestimmte(n) Server oder Einheit anfordern.
- Sich selbst oder jemand anderen für ein Zertifikat vorab registrieren, das den Zugriff auf PKIX-kompatible Anwendungen ermöglicht.

  Später kann die betreffende Person das Zertifikat herunterladen, indem sie der Trust Authority-Client-Anwendung auf ihrer Datenstation die entsprechenden Informationen zur Verfügung stellt.

Die Daten aus den Registrierungsformularen werden in Datenbanksätzen gespeichert, die von den Registratoren der Registrierungsstelle (RA) auf dem Desktop der Registrierungsstelle (RA Desktop) von Trust Authority angezeigt werden können.

Vorabregistrierung

Trust Authority ermöglicht es Programmen oder Administratoren, zukünftige Benutzer vorab zu registrieren.

Wenn Sie andere Personen für Zertifikate vorab registrieren wollen, befolgen Sie die Anweisungen des folgenden Szenarios:

- Sie benötigen Informationen zu der Person, die Sie vorab registrieren wollen. Entweder fragen Sie die betreffende Person selbst, oder Sie ziehen Aufzeichnungen des Unternehmens heran wie beispielsweise Informationen aus einer Datenbank.
- Sie greifen über Ihren Web-Browser auf die Registrierungsseite zu. Es gibt ein eigenes Registrierungsformular für die Vorabregistrierung.
- Sie füllen das Formular mit den Informationen aus, die jeweils auf die Person und den Zertifikatstyp zutreffen. Anschließend übergeben Sie das Formular.
- Sie überprüfen den Status der Anforderung.

  Wenn die Vorabregistrierungsanforderung genehmigt wird, erhalten Sie eine Transaktions-ID, ein Kennwort und die URL der RA, die die Anforderung genehmigt hat.
- Diese Informationen teilen Sie der vorab registrierten Person mit — per Telefon, E-Mail oder persönlich. Um es für die betreffende Person besonders einfach zu machen, haben Sie auch die Möglichkeit, ihr eine Vorabregistrierungsdatei zur

Verfügung zu stellen, in der weitere Anforderungsinformationen enthalten sind. Wenn die Person bereit ist, ihr Zertifikat anzufordern, verwendet sie die von Ihnen gelieferten Informationen.

Wenn Sie selbst ein vorab registrierter Benutzer sind, befolgen Sie die Anweisungen des folgenden Szenarios, um Ihr Zertifikat abzurufen:

- Per Telefon, E-Mail oder persönlich erhalten Sie die Informationen, die Sie benötigen, um Ihr Zertifikat anfordern zu können. Entweder erhalten Sie eine Transaktions-ID, ein Kennwort und die URL der RA, die die Anforderung genehmigt hat, oder Sie erhalten eine Vorabregistrierungsdatei und ein Kennwort.
- Das Zertifikat fordern Sie über die Client-Anwendung an. Wenn Sie dazu aufgefordert werden, geben Sie die Informationen an, die Sie zuvor erhalten haben.
- Während der Verarbeitung Ihrer Zertifikatsanforderung wird die Anforderung im Fenster der Client-Anwendung angezeigt, zusammen mit allen Zertifikaten, die bereits auf der geöffneten Smart Card vorhanden sind.
- Wenn das Zertifikat fertiggestellt ist, wird es über die Client-Anwendung gesendet. Die Client-Anwendung speichert es dann automatisch auf Ihrer Smart Card. Die Anzeige informiert Sie darüber, daß Sie nun im Besitz des Zertifikats sind.

Web-Browser-Unterstützung

Mit Trust Authority können Sie eine Registrierungsanforderung erstellen, indem Sie ein Registrierungsformular ausfüllen und über einen der beiden folgenden Web-Browser übergeben:

- Microsoft Internet Explorer, Release 4.0 oder höher.
- Netscape Navigator oder Communicator, Version 3.0 oder höher.

Registrierung

Die Registrierung ist der Prozeß, über den ein digitales Zertifikat genehmigt und an eine Person oder andere Entität ausgestellt wird. Bei Trust Authority wertet ein Programm oder ein Registrator vor der Registrierung die Informationen aus, die zusammen mit der Registrierungsanforderung zur Verfügung gestellt wurden. Unabhängig davon, ob die Anforderung genehmigt wird oder nicht, erstellt die Trust Authority-Registrierungsstelle (RA) in der Registrierungsdatenbank einen Datensatz für die entsprechende Anforderung. Wenn entschieden wird, das Zertifikat zu genehmigen, wird es vom Trust Authority-Zertifikatsaussteller (CA) ausgestellt.

Unternehmensregeln

Wenn ein Programm oder ein Registrator Ihre Angaben zur Registrierung auswertet, werden auf einige dieser Registrierungsinformationen zur Registrierung die Regeln Ihres Unternehmens angewandt. Die Art der Informationen, die ein Programm auswerten kann, ist weniger komplex als die Informationen, die von einem Registrator ausgewertet werden können. Es handelt sich normalerweise um präzise Werte wie beispielsweise die Mindestanzahl der an einem Wohnort verbrachten Jahre. Mit Trust Authority kann Ihr Unternehmen einem solchen Programm die entsprechenden Informationen zu den Unternehmensregeln zur Verfügung stellen. Das Programm verwendet diese Informationen dann bei der Auswertung.

Registrierungsstellen (RAs)

Bei Trust Authority handelt es sich bei den RAs um eine Server-Anwendung. Sie führt einige der Verwaltungs-Tasks aus, die für die Registrierung von Benutzern erforderlich sind. Dazu gehört unter anderem folgendes:

- Die Identität eines Benutzers bestätigen.
- Überprüfen, ob der Absender der Anforderung Anspruch auf ein Zertifikat mit den angeforderten Attributen und Berechtigungen hat.
- Anforderungen genehmigen oder zurückweisen, um Zertifikate zu erstellen bzw. zu widerrufen.
- Überprüfen, ob eine Person, die versucht, auf eine gesicherte Anwendung zuzugreifen, über den privaten Schlüssel verfügt, der dem öffentlichen Schlüssel im Zertifikat zugeordnet ist.

Registrierungsdatenbanken

Eine Trust Authority-Registrierungsdatenbank speichert Registrierungssätze. Bei der Registrierungsdatenbank handelt es sich um eine relationale Datenbank, die mit IBM DB2 Universal Database erstellt wurde. Die Sätze werden von Trust Authority verschlüsselt. Über den RA Desktop kann ein authorisierter Registrator jedoch die meisten der Registrierungsinformationen lesen.

Registrierungsdomänen

Jedes Trust Authority-System verfügt über eine eigene Registrierungsdomäne. Diese Domäne definiert die Unternehmensregeln, Zertifikatsregeln und Ressourcen, die mit der Registrierung und Zertifizierung in Ihrem Unternehme in Zusammenhang stehen. Benutzer, die auf eine Ressource zugreifen wollen, müssen für die Domäne dieser Ressource registriert sein.

Wenn die RA-Server-Software installiert ist, enthält sie das Gerüst, mit dem ein Unternehmen eine Registrierungsfunktion aufbauen kann. Sie kann alle Sprachen und Regeln verwenden, die von der Registrierungsstelle (RA) unterstützt werden. Der Domänenname, die Sprache und der Installationspfad bilden die URL für den Zugriff auf ein bestimmtes Exemplar der Registrierungsfunktion.

Beispiel: Wenn der Name Ihres öffentlichen Web-Servers 'Mein_öffentlicher_Web-Server' (MyPublicWebServer) und der Name Ihrer Domäne 'Meine_Domäne' (MyDomain) lautet, würden Sie für den Zugriff auf die Registrierungsfunktion die folgende URL verwenden:

```
http://MyPublicWebServer/MyDomain/index.jsp
```

Ein Trust Authority-System enthält eine standardmäßige Java-Server-Seite (index.jsp) mit der entsprechenden Registrierungsfunktion. Diese Seite wird über die Registrierungs-URL Ihrer Registrierungsdomäne angezeigt. Sie stellt die folgenden Registrierungsservices zur Verfügung:

- Potentielle Benutzer rufen diese Web-Seite auf, um ein Zertifikat anzufordern und um ihre eigenen Browser-Zertifikate zu erneuern oder zu widerrufen.
- Administratoren können die Registrierungs-Web-Seite auch dazu aufrufen, um andere Benutzer vorab zu registrieren.

Trust Authority-Registratoren greifen auf den RA Desktop zu, um mit den Registrierungsanforderungen und Zertifikaten zu arbeiten, die einer Registrierungsdomäne zugeordnet sind.

Registrierungssätze

Jede Anforderung für ein Zertifikat ist ein Registrierungsformular, das an die Trust Authority-RA übergeben wird. Jede Registrierungsanforderung führt zu einem Satz in der Registrierungsdatenbank. Aktualisierungen an diesem Satz spiegeln jede für die Anforderung ausgeführte Aktion wider, selbst eine Zurückweisung der Anforderung. Wenn ein Zertifikat erstellt wird, spiegelt derselbe Satz alle Ereignisse wider, die mit diesem Zertifikat in Zusammenhang stehen. Demnach enthält der Registrierungssatz alle Ereignisse im Verarbeitungszyklus der Anforderung und des zugeordneten Zertifikats.

Datensatzeigenschaften

Die Attribute eines Satzes in der Registrierungsdatenbank sind Variablen, die die Registrierungsanforderung beschreiben. Bei ausgeführten Anforderungen beschreiben die Variablen auch das genehmigte Zertifikat. Andere Attribute sind Verarbeitungsvariablen, die Ihrem Unternehmen dabei helfen, ihre Unternehmensregeln umzusetzen. Viele Attribute und ihre zugehörigen Werte können von den Registratoren über den RA Desktop angezeigt werden.

Zertifizierung

Zertifizierung bedeutet die Erstellung eines digitalen Zertifikats für eine Entität oder eine Person. Bei Trust Authority erfolgt die Zertifizierung erst nach der Überprüfung und Genehmigung einer Registrierungsanforderung. Infolge der Registrierung stellt der Zertifikatsaussteller (CA) die Zertifikate aus. Bei Trust Authority stimmt der ausgestellte Zertifikatstyp mit den Regeln Ihres Unternehmens überein.

Zertifikatsaussteller

Bei Trust Authority ist der Zertifikatsaussteller (CA) ein Server-Programm, das für das Ausstellen digitaler Zertifikate verantwortlich ist, die mit den Regeln Ihres Unternehmens übereinstimmen.

Trust Authority unterstützt die gegenseitige Zertifizierung, bei der CAs, die sich gegenseitig vertrauen, die Zertifikate des jeweils anderen CA als Authentizitätsnachweis akzeptieren. Trust Authority unterstützt ebenfalls eine CA-Hierarchie. CAs vertrauen den CAs, die in der Hierarchie über ihnen stehen, und akzeptieren die Zertifikate dieser CAs als Authentizitätsnachweise.

Zertifikatswiderrufslisten (CRL)

Die Trust Authority-RA veröffentlicht in regelmäßigen Abständen eine Zertifikatswiderrufsliste (CRL). Sie enthält die Zertifikate, die nicht mehr gültig sind, damit Inhaber solcher Zertifikate, die diese vorlegen, nicht authentifiziert werden.

Alle CAs, RAs und Anwendungen können auf diese Liste zugreifen, um festzustellen, ob ein Zertifikat widerrufen wurde oder nicht. Dies ist eine Maßnahme, mit der die Trust Authority-RA für Sicherheit sorgt, wenn Benutzer versuchen, auf die gesicherten Anwendungen Ihres Unternehmens zuzugreifen.

Verzeichnisse

Als Verzeichnis zur Speicherung von Zertifikaten verwendet Trust Authority das IBM SecureWay Directory. Dieses Directory kann ein Verzeichnis sein, das Ihr Unternehmen speziell zur Verwendung mit Trust Authority definiert hat. Es kann sich auch um ein Verzeichnis handeln, das Sie zuvor installiert haben und mit anderen Anwendungen verwenden.

Für den Zugriff auf das Directory verwendet Trust Authority das Lightweight Direct Access Protocol (LDAP), ein Direktzugriffsprotokoll mit reduziertem Funktionsumfang.

Registrierter Name

Der registrierte Name (DN, Distinguished Name) ist ein Element des Directory-Eintrags für ein digitales Zertifikat. Er identifiziert eindeutig die Position eines Eintrags in der hierarchischen Struktur des Directory.

Zertifikate

Ein Zertifikat ist ein digitaler Identitätsnachweis, der von einem CA unterzeichnet ist, der für die Identität des Zertifikatsinhabers garantiert. Der Inhaber kann das Zertifikat zur Authentifizierung verwenden, wenn er mit anderen kommuniziert oder wenn er den Zugriff auf eine gesicherte Anwendung anfordert. Bei Trust Authority müssen selbst Server, Anwendungen und Einheiten wie Drucker und Smart Cards über Zertifikate verfügen, um sich gegenüber von Benutzern und gegenseitig zu authentifizieren.

Trust Authority unterstützt X.509v3-Zertifikate in den folgenden Kategorien:
- Browser-Zertifikate
- Server-Zertifikate
- Einheitenzertifikate
- Zertifikate für den Zugriff auf PKIX-kompatible Anwendungen
- Gegenseitig ausgestellte Zertifikate für CAs

Trust Authority unterstützt außerdem die folgenden Protokolle:
- SSL
- S/MIME
- IPSec
- PKIX CMP

Eine standardmäßige Trust Authority-Installation stellt eine Reihe von verschiedenen Zertifikatstypen zur Verfügung, die auf diesen Kategorien und Protokollen basieren. Registrierte Benutzer können ihrem Bedarf entsprechende Zertifikate anfordern. Im Abschnitt „Verfügbare Zertifikatstypen" auf Seite 36 werden die Zertifikatstypen beschrieben.

Browser-Zertifikate

Ein Browser-Zertifikat ist ein digitaler Identitätsnachweis, der normalerweise in einer verschlüsselten Datei von Ihrem Web-Browser gespeichert wird. Einige Anwendungen erlauben die Speicherung der Schlüssel auf einer Smart Card oder einem anderen Datenträger. In einem Trust Authority-System können Sie ein Browser-Zertifikat direkt über Ihren Web-Browser anfordern. Zu einem späteren Zeitpunkt können Sie gegebenenfalls zur Web-Seite zur Registrierung zurückkehren, um dieses Zertifikat zu erneuern oder zu widerrufen.

CA-Zertifikate

Alle Browser, Server, Einheiten und Anwendungen, die über ein Zertifikat zur Vorlage bei Trust Authority-Servern verfügen, müssen ebenfalls ein kompatibles CA-Zertifikat besitzen. Dieses Zertifikat ist erforderlich, um die Datenfernverarbeitung von Servern zu authentifizieren, die im Besitz von Zertifikaten sind, die vom Trust Authority-CA ausgestellt sind.

Ihr Browser muß über ein Trust Authority-CA-Zertifikat verfügen, damit Sie die gesicherten Trust Authority-Registrierungsservices verwenden können. Sie können dieses Zertifikat abrufen, wenn Sie die Web-Seiten von Trust Authority zur Registrierung das erste Mal besuchen. Wann immer Sie danach ein Zertifikat von den Registrierungsservices anfordern, können Sie ein entsprechendes CA-Zertifikat herunterladen, das mit dem angeforderten Zertifikat kompatibel ist.

Beispiel: Wenn Sie ein zweijähriges SSL-Browser-Zertifikat anfordern, können Sie ein CA-Zertifikat herunterladen, das mit diesem Zertifikat kompatibel ist.

Anmerkung: Frühere Releases von Netscape konnten ein Site-Zertifikat akzeptieren, das von einem Trust Authority-Server vorgelegt wurde. Dieses Zertifikat war für Kommunikationen mit dem Server akzeptabel, die entweder von der Server-Seite oder von der Client-Seite authentifiziert wurden. Das neueste Release von Netscape erfordert für Sitzungen, die von der Client-Seite authentifiziert wurden, nun jedoch ein CA-Zertifikat.

Server- und Einheitenzertifikate

Wenn dies im Rahmen Ihrer Tätigkeit erforderlich ist, können Sie ein Zertifikat für einen Server oder eine Einheit anfordern. Verwenden Sie dazu das Registrierungsformular, das über Ihren Web-Browser zur Verfügung gestellt wird.

Der Server oder die Einheit, für den bzw. die Sie ein Zertifikat anfordern, muß das Anforderungsformat PKCS #10 verwenden.

Zertifikatserweiterungen

Zertifikatserweiterungen sind wahlfreie Elemente im Format eines X.509v3-Zertifikats. Die Erweiterungen ermöglichen es, dem Zertifikat weitere Felder hinzuzufügen. Trust Authority stellt eine Gruppe von Zertifikatserweiterungen zur Verfügung, um Ihr Unternehmen in die Lage zu versetzen, die von ihm ausgestellten Zertifikate anzupassen. Diese zusätzlichen Felder werden *Geschäftsprozeßvariablen* genannt.

Zertifikatsverarbeitungszyklus

Wenn Sie ein Zertifikat anfordern, leiten Sie einen Verarbeitungszyklus ein, der sich über die gesamte Laufzeit dieses Identitätsnachweises erstreckt. Dieser Verarbeitungszyklus endet, wenn das Zertifikat widerrufen wird oder abläuft.

Wenn ein Zertifikat erneuert wird, wird ein neuer Datensatz in der Registrierungsdatenbank erstellt.

Erneuerbarkeit

Die Erneuerbarkeit ist eine der Eigenschaften eines Zertifikats, die der Registrator für Sie über den RA Desktop ändern kann:

- Wenn Ihr Zertifikat erneuerbar ist, können Sie ein neues Zertifikat beantragen, während das alte noch gültig ist. Der Besitz eines erneuerbaren Zertifikats vereinfacht den Registrierungsprozeß und verringert den Registrierungsaufwand.
  - Wenn Sie über ein erneuerbares Browser-Zertifikat verfügen, können Sie dessen Erneuerung auf der Registrierungs-Web-Seite anfordern.
  - Wenn Sie über ein erneuerbares Zertifikat für den Zugriff auf eine PKIX-kompatible Anwendung verfügen, können Sie dessen Erneuerung mit Hilfe der Client-Anwendung anfordern.

- Wenn Ihr Zertifikat nicht erneuerbar ist, müssen Sie warten, bis es abläuft, und sich dann erneut registrieren, falls Sie weiterhin ein Zertifikat benötigen. Wenn Sie sich registrieren, müssen Sie alle Informationen zur Verfügung stellen, die Sie auch bei der ersten Registrierung angegeben haben.

Zugriff auf gesicherte Ressourcen

Dieser Abschnitt erläutert die Verwendung und Verwaltung von Zertifikaten.

Zugriffssteuerung

Eine Zugriffssteuerungsliste (ACL, Acces Control List) authentifiziert und genehmigt interne Trust Authority-Benutzer, -Einheiten und -Software. Beispiel: Das RA Desktop-Unterstützungs-Servlet verwendet die ACL, um Registratoren zu authentifizieren und zu genehmigen, bevor diese auf den RA Desktop zugreifen können.

Authentifizierung und Genehmigung

Bei der Authentifizierung wird eine Identität überprüft, während eine Genehmigung die Berechtigung für eine Aktion ist. Trust Authority ermöglicht es Ihrem Unternehmen, sowohl eine Authentifizierung als auch eine Genehmigung zu verlangen, bevor Benutzer auf gesicherte Anwendungen zugreifen können. Im Gegenzug können Zertifikatsinhaber darauf vertrauen, daß die von ihnen genutzten Anwendungen auch sicher sind.

Digitale Unterschriften

Mit Hilfe eines Ihrer Zertifikate können Sie eine Datei mit einer digitalen Unterschrift versehen. Diese Unterschrift sagt dem Empfänger einer Datei beim Öffnen, ob deren Inhalt seit der Unterzeichnung geändert worden ist. Mit der digitalen Unterschrift wird der Inhalt der Datei nicht verschlüsselt.

Smart Cards

Smart Cards sind Speichereinheiten, in denen digitale Identitätsnachweise sicher aufbewahrt werden können. Es gibt virtuelle Smart Cards, die sich auf Ihrer Datenstation befinden, und physische Smart Cards, die entweder intern oder extern sein können. Sie können eine externe Smart Card von Maschine zu Maschine mitnehmen, doch ist sie aufgrund ihrer Übertragbarkeit weniger sicher.

Wenn Sie über die Client-Anwendung ein neues Zertifikat herunterladen, wird es automatisch auf der Smart Card gespeichert, die Sie geöffnet haben.

Kapitel 5. Referenzinformationen

Die folgenden Abschnitte enthalten Feldbeschreibungen, zulässige Feldwerte und die Bedeutung der Zertifikatsattribute. Ebenso enthalten sind Informationen, die Ihnen bei der Verwendung von Trust Authority in einer anderen Sprache als Englisch helfen können.

Registrierungsformular auf der Web-Seite

Das Registrierungsformular enthält Abschnitte für Daten über den potentiellen Zertifikatsinhaber und für Daten über die Anforderung des Zertifikats. Einige Felder in diesen Abschnitten stehen nur für bestimmte Registrierungsarten zur Verfügung.

Anmerkung: Wenn Ihr Unternehmen die Registrierungsformulare anpaßt, kann deren Inhalt von der Beschreibung in diesem Handbuch abweichen.

Die **Registrierungsinformationen** enthalten die folgenden Felder, sofern sie auf den angeforderten Zertifikatstyp zutreffen:

Zertifikatstyp
Wählen Sie einen Wert aus der Liste aus. Im Abschnitt „Verfügbare Zertifikatstypen" auf Seite 36 werden die Zertifikatstypen beschrieben, die mit einer Standardinstallation zur Verfügung gestellt werden.

Vorname
Geben Sie in dieses Feld Ihren Vornamen ein. Die Angabe eines zweiten Vornamens oder dessen Anfangsbuchstabens steht Ihnen frei.

Bei einer Vorabregistrierung beziehen sich diese Angaben auf die Person, die Sie vorab registrieren.

Nachname
Geben Sie in dieses Feld Ihren Nachnamen oder Familiennamen ein.

Bei einer Vorabregistrierung beziehen sich diese Angaben auf die Person, die Sie vorab registrieren.

E-Mail-Adresse
Geben Sie in dieses Feld Ihre E-Mail-Adresse ein, einschließlich des kommerziellen A (@) und aller Punkte (.). Für einige Zertifikatstypen (beispielsweise Zertifikate für sichere E-Mails) ist diese Adresse erforderlich. Um **E-Mail-Benachrichtigung** auswählen zu können, müssen Sie eine E-Mail-Adresse angeben.

E-Mail-Benachrichtigung
Wählen Sie diese Option aus, um per E-Mail vom Ergebnis der vorliegenden Registrierungsanforderung benachrichtigt zu werden.

Anmerkung: Wenn der RA-Server auf einer Windows NT-Plattform in Ihrem Unternehmen installiert ist, muß die Konfigurationsdatei (raconfig.cfg) der Registrierungsfunktion möglicherweise aktualisiert werden, damit sie auf einen SMTP-Host verweist, um diese Funktion zu aktivieren. Das Handbuch *Trust Authority Anpassung* enthält weitere Informationen hierzu.

Identifikationsprüfungsfrage
Dies ist eine Frage, deren Antwort nur Sie kennen und die verwendet werden kann, um Ihre Identität zu überprüfen bzw. um zu verhindern, daß sich jemand anderes für Sie ausgibt. Wenn Sie den Status der Registrierungsanforderung überprüfen, wird Ihnen diese Frage gestellt. Sie müssen die Identifikationsprüfungsfrage beantworten, unabhängig davon, ob die Anforderung für Sie selbst, für einen Server oder eine Einheit oder zur Vorabregistrierung einer anderen Person gestellt wird.

Identifikationsprüfungsantwort
Dies ist die Antwort auf die Identifikationsprüfungsfrage, die Sie angegeben haben. Geben Sie eine Antwort ein, die leicht zu merken ist. Wenn Sie den Status Ihrer Anforderung überprüfen, müssen Sie genau dieselbe Antwort eingeben.

Anmerkung: Bei der Antwort ist die Groß-/Kleinschreibung zu beachten.

Kennwort
(*Nur Vorabregistrierung*) Dies ist das Kennwort, das die von Ihnen vorab registrierte Person der Client-Anwendung zur Verfügung stellen muß, wenn sie bereit ist, das Zertifikat herunterzuladen. Verwenden Sie die Zeichen A-Z, a-z und 0–9. Das Kennwort darf zwischen 8 und 32 Zeichen enthalten.

Wenn Sie kein Kennwort angeben, generiert die Registrierungsfunktion für Sie ein Kennwort, das 10 Zeichen enthält. Bei Genehmigung der Vorabregistrierungsanforderung erhalten Sie dieses Kennwort zusammen mit einer Transaktions-ID.

Kennwort bestätigen
(*Nur Vorabregistrierung*) Geben Sie dasselbe Kennwort nochmals ein.

Die **Zertifikatsanforderungsinformationen** enthalten die folgenden Felder:

PKCS #10-Zertifikatsanforderung
(*Nur Server- oder Einheitenregistrierung*) Dieses Feld ist für den Inhalt der PKCS #10-Zertifikatsanforderung, die von dem Server bzw. der Einheit generiert wurde, für den bzw. die Sie ein Zertifikat anfordern. Wenn die Anforderung in einer Datei gespeichert wurde, öffnen Sie die Datei mit einem Texteditor wie beispielsweise Windows Notepad. Kopieren Sie den Inhalt, und fügen Sie ihn in das Textfenster des Registrierungsformulars ein.

Allgemeiner Name
Dies ist ein Name zur Identifizierung dieses Zertifikats.

- Bei Personen ist dies normalerweise der vollständige Name der betreffenden Person.
- Bei Servern oder Einheiten ist dies gewöhnlich der Host-Name. Sie müssen diesen Wert eingeben, wenn im Feld für die PKCS #10-Zertifikatsanforderung kein Host-Name vorhanden ist.

Schlüsselgröße
(*Nur Netscape-Browser-Registrierung*) Dies ist die Schlüsselgröße für das Schlüsselpaar aus öffentlichem und privatem Schlüssel. Wählen Sie einen Wert aus. Größere Schlüssel sind sicherer, verlängern jedoch auch die Zeit, die erforderlich ist, um eine Verbindung zu einer sicheren Sitzung herzustellen.

Verschlüsselungsserviceanbieter
(*Nur Internet Explorer-Browser-Registrierung*) Dies ist der Verschlüsselungsserviceanbieter (Cryptographic Service Provider, CSP), der Ihr Schlüsselpaar aus öffentlichem und privatem Schlüssel generieren soll. Wählen Sie einen Wert aus. Größere Schlüssel sind sicherer, verlängern jedoch auch die Zeit, die erforderlich ist, um eine Verbindung zu einer sicheren Sitzung herzustellen.

Die Standardeinstellung ist Microsoft Base Cryptographic Provider. Dieser Verschlüsselungsserviceanbieter stellt Schlüssel mit 512 Bit für die Verschlüsselung zur Verfügung.

Microsoft Enhanced Cryptographic Provider (sofern auf Ihrem System installiert) stellt Schlüssel mit 1024 Bit zur Verfügung.

Schlüsselsatz
(*Nur Internet Explorer-Browser-Registrierung*) Dies ist das zu verwendende Schlüsselpaar. Wählen Sie **Neuen Schlüsselsatz generieren** aus, oder öffnen Sie die Liste, und wählen Sie eines der vorhandenen Schlüsselpaare aus.

Name des neue Schlüsselsatzes
(*Nur Internet Explorer-Browser-Registrierung*) Dies ist der Name des neuen Schlüsselsatzes, der generiert werden soll. Sie können dieses Feld auch leer lassen und eine GUID (Globally Unique Identifier) für den Namen generieren lassen. In diesem Fall ist es jedoch schwieriger, das Schlüsselpaar wiederzuerkennen.

Zusätzliche Sicherheitsoptionen
Dies sind zusätzliche Sicherheitsfunktionen, die Microsoft Internet Explorer für Ihr neues Schlüsselpaar zur Verfügung stellt. Wenn Sie diese Option auswählen, zeigt ihr Web-Browser unmittelbar nach Übergabe dieses Registrierungsformulars entsprechende Internet Explorer-Dialoge an, mit denen Sie diese Optionen einstellen können.

Firmenname
Dies ist der gesetzlich registrierte Name Ihrer Firma.

Abteilung
Dies ist der Name Ihrer Abteilung, beispielsweise Personalabteilung oder Softwareentwicklung.

Adresse
Dies ist die Adresse (Straße, Hausnummer) Ihres Unternehmens.

Ort Dies ist die Stadt, in der Ihr Unternehmen ansässig ist, beispielsweise Chicago oder Berlin.

Bundesland
Dies ist das Bundesland, in dem Ihr Unternehmen ansässig ist. Ob Sie den vollständigen Namen des Bundeslandes schreiben oder eine offizielle Abkürzung verwenden, hängt von Ihren Registrierungsregeln ab.

Land Dies ist das Land, in dem Ihr Unternehmen ansässig ist. Wählen Sie einen Wert aus.

Domänenname
Der Host-Name der Maschine, auf der ein Zertifikat installiert wird. Für Server-Zertifikate und Endbenutzerzertifikate (Browser-Zertifikate und Zertifikate, die über die Vorabregistrierung für die Trust Authority-Client-Anwendung abgerufen werden) ist dieses Feld wahlfrei. Wenn Sie dieses Feld integrieren wollen, müssen Sie die Maschine identifizieren, auf der

der Browser, der Client oder der Web-Server installiert ist. Für IPSec-Zertifikate müssen Sie die IPSec-Einheit identifizieren, auf der das Zertifikat installiert wird.

Verfügbare Zertifikatstypen

Ein Trust Authority-System stellt mehrere Zertifikatstypen für die unterstützten Zertifikatskategorien und -protokolle zur Verfügung. Zu den Abwandlungen gehören verschiedene Gültigkeitszeiträume. Der Name des Zertifikats zeigt an, wie lange es gültig ist und wofür der Schlüssel hauptsächlich verwendet wird. Das Glossar enthält eine Beschreibung der jeweiligen Funktionen.

Gegenseitig ausgestelltes CA-Zertifikat
Mit diesem Zertifikat kann der Zertifikatsaussteller (CA), dem dieses Zertifikat gehört, seine Zertifikate vom ausstellenden CA genehmigen lassen. Das Zertifikat stellt die Funktionen für digitale Unterschriften und Unbestreitbarkeit zur Verfügung.

Datenverschlüsselungszertifikat - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann der Inhaber Daten verschlüsseln. Das Zertifikat ist nicht für andere Zwecke gedacht.

E-Mail-Schutzzertifikat - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann der Inhaber das S/MIME-Protokoll (Secure Multi-Purpose Internet Mail Exchange) verwenden. Dieses Protokoll schützt E-Mail und andere MIME-Objekte. Es stellt die Funktionen für die Authentifizierung des Absenders, Nachrichtenintegrität, Unbestreitbarkeit des Absenders und Vertraulichkeit zur Verfügung. Es wird normalerweise von Endbenutzer gewählt.

IPSec-Zertifikat - 1 Jahr und 2 Jahre
Dieses Zertifikat gewährleistet die Integrität und Vertraulichkeit von Daten, die in IP-Paketen (IP = Internet Protocol) über das Internet gesendet werden. IPSec-Zertifikate sind eher für Daten als für Benutzer gedacht. Sie sind häufig einem Router zugeordnet.

Zertifikat für Schlüsselcodierung (ausschließlich) - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann der Inhaber Schlüssel codieren. Das Zertifikat ist nicht für andere Zwecke gedacht.

Unbestreitbarkeitszertifikat - 1 Jahr und 2 Jahre
Dieses Zertifikat stellt die Funktionen für Nachrichtenverschlüsselung und digitale Unterschriften zur Verfügung, um die Unbestreitbarkeit des Nachrichtenabsenders bzw. die Unbestreitbarkeit der Nachrichtenzustellung zu gewährleisten.

Zertifikat für Unterschrift (ausschließlich) - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann der Inhaber Dateien digital unterzeichnen. Das Zertifikat ist nicht für andere Zwecke gedacht.

Web-Client-Authentifizierungszertifikat - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann ein Web-Browser an einer vom Client authentifizierten SSL-Sitzung teilnehmen. Der Benutzer des Browsers kann mit diesem Zertifikat auf eine spezifische gesicherte Web-Site zugreifen. Das Zertifikat stellt die Funktionen für digitale Unterschriften, Unbestreitbarkeit und Schlüsselcodierung zur Verfügung. Es wird normalerweise vom Endbenutzer gewählt.

Web-Server-Authentifizierungszertifikat - 1 Jahr und 2 Jahre
Mit diesem Zertifikat kann ein Server an einer vom Server authentifizierten SSL-Sitzung teilnehmen. Das Zertifikat stellt die Funktionen für digitale Unterschriften und Schlüsselcodierung zur Verfügung.

Registrierte Personen oder Personen, die jemand anderen vorab registrieren, können einen geeigneten Zertifikatstyp anfordern. Die verfügbaren Zertifikatstypen werden in den Registrierungsformularen im Feld **Zertifikatstyp** aufgelistet. In der Client-Anwendung werden die Zertifikatstypen im Feld **Zweck** der jeweiligen Zertifikatsbeschreibung aufgelistet.

Anmerkung: Die angezeigte Liste entspricht unter Umständen nicht der Liste in diesem Handbuch. Es kann sein, daß Ihr Unternehmen die Namen oder sogar die verfügbaren Zertifikatstypen geändert hat.

Begründung für den Widerruf von Zertifikaten

Wenn Sie ein Zertifikat widerrufen, müssen Sie dafür eine Begründung auswählen. Die folgenden Begründungen sind zulässig und können ausgewählt werden:

Der CA-Schlüssel war beschädigt
Der Schlüssel des Zertifikatsausstellers (CA), der das Zertifikat ausgestellt hat, wurde beschädigt.

Das Zertifikat wurde ersetzt
Sie haben ein neues Zertifikat und benötigen das vorliegende nicht mehr.

Keine Begründung
Sie geben keine Begründung an.

Der ursprüngliche Verwendungszweck des Zertifikats ist nicht mehr gültig
Sie benötigen das Zertifikat nicht mehr für dessen ursprünglichen Verwendungszweck. Beispiel: Sie müssen nicht mehr auf die Ressource oder die Anwendung zugreifen, für die das Zertifikat ausgestellt wurde.

Benutzer hat Zugehörigkeit geändert
Sie arbeiten nicht mehr mit dem Unternehmen zusammen, für das das Zertifikat gilt.

Der Benutzerschlüssel war beschädigt
Ihr privater Schlüssel wurde beschädigt.

Anmerkung: Die folgenden Begründungen führen zu Änderungen der Widerrufsaktion:

Zertifikat in den Wartestatus setzen
Hiermit inaktivieren Sie ein Zertifikat, anstatt es permanent zu widerrufen. Wenn Sie das Zertifikat wieder verwenden wollen, bitten Sie den Registrator, es erneut zu aktivieren. Wenn das Zertifikat jedoch abläuft, während es sich auf der Zertifikatswiderrufsliste (CRL) befindet, können Sie es nicht erneut aktivieren.

Anmerkung: Auf den Registrierungsformularen werden die zulässigen Begründungen im Feld **Begründung** aufgelistet, wenn Sie ein Zertifikat auf der Registrierungs-Web-Seite widerrufen. Bei der Client-Anwendung werden sie im Feld **Begründung für den Widerruf** des Dialogs 'Zertifikat widerrufen' aufgelistet. Auf Seite 21 wird dieser Dialog beschrieben.

Systemvoraussetzungen für die Browser-Registrierung

Für die Verwendung der Browser-Registrierungsformulare mit der Registrierungsfunktion empfiehlt IBM die folgende Datenstationskonfiguration.

- Konfiguration der physischen Maschine:
  - Intel 486-Prozessor mit 166 MHz und 32 MB RAM als Mindestanforderung (Vorzugsweise Intel Pentium-Prozessor mit 200 MHz und mindestens 64 MB RAM)
  - Computer-Bildschirm, der mindestens VGA-Auflösung unterstützt
- Eines der folgenden Betriebssysteme:
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT
- Einen der folgenden Web-Browser:
  - Netscape Navigator oder Netscape Communicator, Version 4.05 oder höher
  - Microsoft Internet Explorer, Version 5.0, mit aktiviertem Java
- Wahlfrei: Unterstützung für eine physische Smart Card. Wenn Sie planen, Zertifikate auf Smart Cards zu speichern, müssen Sie Ihren Browser möglicherweise mit einer für die entsprechende Smart Card erforderlichen Version aktualisieren. Beispiel: IBM SecureWay Smart Card Security Kit erfordert einen der folgenden Browser:
  - Netscape Navigator oder Netscape Communicator, Version 4.6 oder höher
  - Microsoft Internet Explorer, Version 5.0 oder höher

Systemvoraussetzungen für die Client-Anwendung

- Sie müssen die Trust Authority Client-Anwendung auf einer Windows NT-Maschine installieren.
- Sie können die Client-Anwendung nicht auf derselben Maschine installieren, auf der die Trust Authority-Server-Programme installiert wurden. Ein Administrator sollte das Installationsabbild als Teil der Trust Authority-Installation auf dem Server installieren, es jedoch nicht auf derselben Maschine ausführen.
- Für die Installation der Client-Anwendung sind mindestens 80 MB freier Plattenspeicherplatz auf dem Festplattenlaufwerk erforderlich, auf dem die temporären Dateien gespeichert werden. Wenn Sie feststellen wollen, um welches Laufwerk es sich dabei handelt, geben Sie den folgenden Befehl ein, mit dem die Umgebungseinstellungen der Variable TEMP überprüft werden:

  ```
  md %temp%
  ```

  Ist ein Verzeichnis TEMP vorhanden, wird vom System die folgende Nachricht angezeigt: "Ein Unterverzeichnis bzw. eine Datei *laufwerk*:\TEMP ist bereits vorhanden." Andernfalls wird das Verzeichnis TEMP vom System erstellt. Bitte beachten Sie, daß das Installationsprogramm temporäre Dateien, die es erstellt, nach der Installation der Client-Anwendung löscht.
- Darüber hinaus sind 60 MB freier Plattenspeicherplatz auf dem Festplattenlaufwerk erforderlich, auf dem die Client-Anwendung installiert werden soll, sowie 0,5 MB freier Plattenspeicherplatz auf dem Festplattenlaufwerk, auf dem das Windows-Betriebssystem installiert ist.
- Um mit der Trust Authority-Client-Anwendung eine physische Smart Card zu verwenden, benötigen Sie eine von der betreffenden Smart Card unterstützte Browser-Version. Beispiel: IBM SecureWay Smart Card Security Kit kann mit folgenden Browsern verwendet werden:
  - Microsoft Internet Explorer, Version 5.0 oder höher
  - Netscape Navigator oder Netscape Communicator, Version 4.6 oder höher

Client-Anwendung - Hauptfenster

Alle Hauptfunktionen der Client-Anwendung stehen im Fenster 'Trust Authority: Smart Card' zur Verfügung.

Menüs im Fenster 'Smart Card'

Die folgenden Menüoption stehen im Fenster 'Smart Card' zur Verfügung. Viele der Optionen erfordern, daß Sie zunächst ein Zertifikat aus den Tabellen unter den beiden Registerkarten unter dem Menü auswählen. Um ein Zertifikat auszuwählen, klicken Sie die entsprechende Zeile in der Tabelle an.

Menü 'Smart Card'

Kennwort ändern
Ändern Sie das Kennwort der geöffneten Smart Card.

Eigenschaften anzeigen
Zeigen Sie die Eigenschaften der geöffneten Smart Card an.

Beenden
Schließen Sie die Client-Anwendung.

Menü 'Zertifikat'

Neu Fordern Sie ein neues Zertifikat an, indem Sie die Daten der Vorabregistrierung verwenden:

- Eine Transaktions-ID
- Eine Vorabregistrierungsdatei

Öffnen
Zeigen Sie Informationen über das ausgewählte Zertifikat an.

Importieren
Importieren Sie das ausgewählte Zertifikat auf die Smart Card.

Exportieren
Exportieren Sie das ausgewählte Zertifikat von einer Smart Card.

Löschen
Löschen Sie das ausgewählte Zertifikat von einer Smart Card.

Erneuern
Erneuern Sie das ausgewählte Zertifikat.

Widerrufen
Widerrufen Sie das ausgewählte Zertifikat.

Unterzeichnen
Verwenden Sie das ausgewählte Zertifikat, um eine Datei digital zu unterzeichnen.

Hilfe

Zu diesem Fenster
Stellt eine Verbindung zum Hilfetext für das aktuelle Fenster her.

Hilfethemen
Zeigt das *Benutzerhandbuch von Trust Authority* an.

Produktinformationen
Zeigt Informationen zur Client-Anwendung an.

Registerkarten im Fenster 'Smart Card'

Unter der Menüleiste verfügt das Fenster über zwei Registerkarten:

Registerkarte 'Meine Zertifikate'
Zeigt eine Tabelle an, in der alle aktuellen Zertifikate, die sich auf der geöffneten Smart Card befinden, sowie alle anstehenden Anforderungen wie beispielsweise Anforderungen neuer Zertifikate und Widerrufsanforderungen aufgelistet sind.

Registerkarte Andere Zertifikate
Zeigt eine Tabelle an, in der Zertifikate aufgelistet sind, die sich auf derselben geöffneten Smart Card befinden, jedoch nicht Ihnen gehören.

Tabellen im Fenster 'Smart Card'

Jede Registerkarte im Fenster 'Smart Card' enthält eine Tabelle, in der die auf der Smart Card befindlichen Zertifikate beschrieben werden. In jeder Zeile wird jeweils ein Zertifikat beschrieben. Die Spalten liefern die folgenden Informationen:

Status Der Status des Zertifikats oder der Anforderung eines Zertifikats. Folgende Werte sind möglich:

Ausgestellt
Die Registrierungsstelle (RA) hat das Zertifikat ausgestellt, und die Client-Anwendung hat es auf der Smart Card gespeichert.

Nicht genehmigt
Die RA hat die Zertifikatsanforderung zurückgewiesen.

Erneuern übergeben
Die Anforderung zur Erneuerung des Zertifikats wurde an die RA gesendet.

Widerrufen übergeben
Die Anforderung zum Widerruf des Zertifikats wurde an die RA gesendet.

Übergeben
Die Zertifikatsanforderung wurde an die RA gesendet.

Kennsatz
Eine eindeutige Beschreibung für das ausgestellte Zertifikat.

Name des Zertifikatsgegenstands
Der registrierte Name des Zertifikats.

Zweck
Die hauptsächliche Verwendung des Zertifikats.

Ablaufdatum
Das Datum, ab dem das Zertifikat nicht mehr gültig ist.

Dialoge der Client-Anwendung

Die Client-Anwendung stellt Dialoge zur Verfügung, in denen Sie während der Arbeit mit Ihren Zertifikaten Einzelangaben machen können. Ausgangspunkt aller Tasks sind die Menüs im Fenster 'Smart Card'. Die Client-Anwendung zeigt dann jeweils den entsprechenden Dialog für die Task an.

Dialog 'Zertifikatserneuerung'

In diesem Dialog können Sie für jedes Zertifikat, das innerhalb des von Ihrem Unternehmen vorgegebenen Intervalls demnächst ablaufen wird, zusammenfassende Informationen anzeigen. Die Standardeinstellung ist 30 Tage. Alle demnächst ablaufenden Zertifikate werden in der Tabelle in einer eigenen Zeile angezeigt.

Die Spalten liefern die folgenden Informationen:

Kennsatz
Eine eindeutige Beschreibung für das ausgestellte Zertifikat.

Seriennummer
Die Seriennummer des Zertifikats.

Zweck
Die hauptsächliche Verwendung des Zertifikats. Dieses Feld enthält einen Zertifikatstyp. Im Abschnitt „Verfügbare Zertifikatstypen" auf Seite 36 werden die für eine Standardinstallation unterstützten Typen aufgelistet.

Ablaufdatum
Das letzte Datum, an dem das Zertifikat noch gültig ist.

Um eines oder mehrere dieser Zertifikate zu erneuern, überprüfen Sie die zusammenfassenden Informationen, wählen Sie die gewünschten Zertifikate aus, und klicken Sie auf **OK**. Wenn Sie keine Auswahl treffen, klicken Sie auf 'OK', um den Dialog zu schließen.

Zugehörige Abschnitte:

„Mehr Zeilen in einer Tabelle anzeigen" auf Seite 22
„Die Größe einer Tabellenspalte ändern" auf Seite 23

Dialog 'Kennwort ändern'

In diesem Dialog können Sie Ihr Kennwort für eine virtuelle Smart Card ändern.

Anmerkung: Um das Kennwort für eine physische Smart Card zu ändern, müssen Sie die Software verwenden, die mit der Smart Card geliefert wurde.

Aktuelles Kennwort
Geben Sie das aktuelle Kennwort für Ihre virtuelle Smart Card ein.

Neues Kennwort
Geben Sie das gewünschte neue Kennwort ein. Das Kennwort kann zwischen 8 und 32 Zeichen enthalten, und zwar A-Z, a-z und 0–9.

Kennwort bestätigen
Geben Sie dasselbe neue Kennwort nochmals ein.

Dialog 'Zertifikat löschen'

In diesem Dialog können Sie zusammenfassende Informationen zu einem der folgenden Einträge anzeigen, den Sie zum Löschen ausgewählt haben:

- Zertifikate, die Sie von der geöffneten Smart Card löschen wollen.
- Anstehende Anforderungen, die Sie zwar übergeben haben, die Sie jedoch stornieren wollen, bevor sie von der RA bearbeitet werden. Alle Arten von anstehenden Anforderungen sind möglich. Es kann sich sogar um eine Anforderung zum Löschen oder Widerrufen eines Zertifikats handeln.

1. Überprüfen Sie die Informationen, die das Zertifikat oder die Anforderung beschreiben. Auf Seite 43 werden die angezeigten Details beschrieben.
2. Wenn Sie den ausgewählten Eintrag tatsächlich löschen wollen, klicken Sie auf **OK**.

Anmerkung: Wenn die anstehende Anforderung, die Sie löschen wollen, nicht angezeigt wird, hat die Anforderung nicht länger den Status 'anstehend' und kann daher nicht mehr gelöscht werden.

Dialog 'Zertifikat exportieren'

In diesem Dialog geben Sie die Informationen ein, die erforderlich sind, um ein Zertifikat von der geöffneten Smart Card in eine Datei zu exportieren.

Verschlüsselungsart
Wählen Sie die Verschlüsselungsstufe für die Datei aus. Eine höhere Verschlüsselungsstufe erfordert einen größeren Schlüssel und nimmt mehr Zeit in Anspruch, um eine sichere Verbindung herzustellen.

Dateiname
Geben Sie den Pfad und Dateinamen an, unter dem das Zertifikat gespeichert werden soll, wenn Sie es von der Smart Card exportieren. Über den Knopf **Anzeigen** können Sie einen Pfad auswählen, bevor Sie den Dateinamen eingeben.

Dateikennwort
Schützen Sie die Datei durch Eingabe eines eigenen Kennworts. Es kann zwischen 8 und 32 alphanumerische Zeichen (A-Z, a-z, 0-9) enthalten.

Dialog 'Zertifikat importieren'

In diesem Dialog geben Sie die Informationen ein, die erforderlich sind, um ein Zertifikat aus einer Datei auf die geöffnete Smart Card zu importieren.

Dateiname
Geben Sie den Pfad und den Namen der Datei ein, in der sich das Zertifikat befindet. Über den Knopf **Anzeigen** können Sie den Pfad und Dateinamen auswählen, anstatt diese Angaben manuell einzugeben.

Dateikennwort
Geben Sie das Kennwort zum Schutz der Datei ein.

Dialog 'Neues Zertifikat unter Verwendung einer Vorabregistrierungsdatei'

In diesem Dialog können Sie sich für ein Zertifikat registrieren lassen, indem Sie eine Vorabregistrierungsdatei und ein Kennwort angeben, die bzw. das Sie vom Administrator, der Sie vorab registriert hat, erhalten haben. Sie haben die Datei und das Kennwort entweder per E-Mail oder auf Diskette erhalten.

Name der Vorabregistrierungsdatei
Geben Sie den Pfad und den Namen der Vorabregistrierungsdatei ein, die Sie erhalten haben. Über den Knopf **Anzeigen** können Sie den Pfad und Dateinamen auswählen, anstatt diese Angaben manuell einzugeben.

Kennwort
Geben Sie das Kennwort ein, das Sie zum Abruf Ihres Zertifikats erhalten haben.

Wenn Ihr Unternehmen die entsprechende Option gewählt hat, werden nach Eingabe des Kennworts die Attribute und Werte angezeigt, die Ihrer Zertifikatsanforderung zugeordnet sind. Einige dieser Werte können unter Umständen bearbeitet werden.

Dialog 'Neues Zertifikat unter Verwendung einer Transaktions-ID'

In diesem Dialog können Sie sich für ein Zertifikat registrieren lassen, indem Sie die Transaktionsdaten verwenden, die Sie vom Administrator, der Sie vorab registriert hat, erhalten haben. Sie haben diese Daten entweder per E-Mail oder Telefonanruf erhalten.

Geben Sie diese Daten in den Dialog ein.

Transaktions-ID
Geben Sie die Transaktions-ID ein, die Sie zum Erstellen des neuen Zertifikats erhalten haben.

Kennwort
Geben Sie das Kennwort ein, das Sie zum Abruf des Zertifikats erhalten haben.

URL der RA
Wählen Sie aus der Liste die URL aus, die Sie erhalten haben, oder geben Sie die entsprechende URL in das Textfenster ein.Beispiel: `pkix://<your server>;<your port>`, wobei folgendes gilt: <*your server*> ist der Host-Name Ihrer RA, und <your port> ist der Anschluß, über den auf die entsprechende URL zugegriffen werden kann.

Schlüsselalgorithmus
Wählen Sie den von Ihrem Unternehmen vorgeschlagenen Verschlüsselungsalgorithmus aus, den Sie für den privaten Schlüssel, der diesem Zertifikat zugeordnet ist, verwenden sollen. Die Werte auf der Liste sind für Ihre Maschine geeignet. Zusammen mit der **Schlüsselgröße** definiert dieser Algorithmus die Stufe des Schlüssels.

Schlüsselgröße
Wählen Sie eine Größe für den privaten Schlüssel aus, der diesem Zertifikat zugeordnet ist. Die Werte auf der Liste sind für Ihre Maschine geeignet. Größere Schlüssel sind sicherer, verlängern jedoch auch die Zeit, die erforderlich ist, um eine Verbindung zu einer sicheren Sitzung herzustellen.

Dialog 'Zertifikat öffnen'

In diesem Dialog können Sie die Details zu dem Zertifikat bzw. der Zertifikatsanforderung anzeigen, das bzw. die Sie im Fenster **'Smart Card'** ausgewählt haben.

Die Beschreibung ist in mehrere Abschnitte aufgeteilt. Die Abschnitte enthalten allgemeine Informationen, Informationen zum Zertifikatsgegenstand und Informationen zum Aussteller. Die Informationen zu einer Zertifikatsanforderung unterscheiden sich in gewisser Weise von denen zu einem Zertifikat. Eine Zertifikatsanforderung hat beispielsweise keine Seriennummer.

Die **allgemeinen Informationen** enthalten folgendes:

Kennsatz
Eine eindeutige Beschreibung für das ausgestellte Zertifikat.

Seriennummer
Die Seriennummer des Zertifikats.

Status Der Status des Zertifikats bzw. der Zertifikatsanforderung.

Gültigkeitsdatum
Das Datum, ab dem das Zertifikat gültig ist.

Zweck
Die hauptsächliche Verwendung des Zertifikats.

Schlüsselalgorithmus
Die ID des Verschlüsselungsalgorithmus für den privaten Schlüssel, der dem Zertifikat zugeordnet ist. Zusammen mit der **Schlüsselgröße** identifiziert dieser Algorithmus die Stufe des Schlüssels.

Schlüsselgröße
Die Länge des privaten Schlüssels, der dem Zertifikat zugeordnet ist.

E-Mail-Adresse
Ihre E-Mail-Adresse im Internet.

Die **Informationen zum Zertifikatsgegenstand** enthalten folgende Angaben zu der Entität, für die das Zertifikat ausgestellt wurde:

Allgemeiner Name
Der Name des Zertifikatsinhabers.

Abteilung
Der Geschäftsbereich, dem der Zertifikatsinhaber angehört.

Firmenname
Das Unternehmen des Zertifikatsinhabers.

Ort Das Bundesland, in dem sich der Zertifikatsinhaber befindet.

Land Das Land, in dem sich der Zertifikatsinhaber befindet.

Die **Informationen zum Aussteller** enthalten die folgenden Angaben über den Zertifikatsaussteller (CA), der das Zertifikat ausgegeben hat:

Allgemeiner Name
Die ID des CA, der das Zertifikat ausgestellt hat.

Abteilung
Der Geschäftsbereich, dem der Aussteller angehört.

Firmenname
Der Name des Unternehmens des Ausstellers.

Ort Das Bundesland, in dem sich der Aussteller befindet.

Land Das Land, in dem sich der Aussteller befindet.

Dialog 'Smart Card öffnen'

In diesem Dialog wählen Sie aus einer Liste die Smart Card aus, die Sie zusammen mit der Client-Anwendung verwenden wollen.

Smart Card
Wählen Sie eine Smart Card aus der Liste aus.

Kennwort
Geben Sie das Kennwort für die ausgewählte Smart Card ein.

Dialog 'Zertifikat erneuern'

In diesem Dialog können Sie zusammenfassende Informationen zu einem Zertifikat anzeigen, um zu überprüfen, ob Sie dieses Zertifikat tatsächlich erneuern wollen.

Wenn Sie sich entschließen, das Zertifikat zu erneuern, dann hat das neue Zertifikat dieselbe Gültigkeitsdauer wie das alte. Sie können entweder das Schlüsselpaar des alten Zertifikats verwenden oder ein neues Schlüsselpaar generieren.

Um das Zertifikat zu erneuern, geben Sie folgende Informationen ein:

URL der RA
Wenn das Feld noch keinen Wert enthält, wählen Sie entweder die URL der RA aus, die die ursprüngliche Zertifikatsanforderung genehmigt hat, oder geben Sie die URL in das Textfenster ein. Wenn Sie die URL nicht kennen, setzen Sie sich mit dem Administrator der Registrierungsdomäne in Verbindung.

Schlüsselalgorithmus
Wenn Sie das Schlüsselpaar des ablaufenden Zertifikats verwenden wollen, ignorieren Sie dieses Feld. Um ein neues Schlüsselpaar zu generieren, wählen Sie einen Wert aus. Die Werte auf der Liste sind für Ihre Maschine geeignet.

Dies ist der Verschlüsselungsalgorithmus für den privaten Schlüssel, der diesem Zertifikat zugeordnet ist. Zusammen mit der **Schlüsselgröße** definiert dieser Algorithmus die Stufe des Schlüssels.

Schlüsselgröße
Wenn Sie das Schlüsselpaar des ablaufenden Zertifikats verwenden wollen, ignorieren Sie dieses Feld. Um ein neues Schlüsselpaar zu generieren, wählen Sie einen Wert aus. Die Werte auf der Liste sind für Ihre Maschine geeignet.

Dies ist die Größe des privaten Schlüssels, der diesem Zertifikat zugeordnet ist. Größere Schlüssel sind sicherer, verlängern jedoch auch die Zeit, die erforderlich ist, um eine Verbindung zu einer sicheren Sitzung herzustellen.

Dialog 'Zertifikat widerrufen'

In diesem Dialog können Sie zusammenfassende Informationen zu einem Zertifikat anzeigen, um zu überprüfen, ob Sie dieses Zertifikat tatsächlich widerrufen wollen.

Um das Zertifikat zu widerrufen, geben Sie folgende Informationen ein:

URL der RA
Wenn das Feld noch keinen Wert enthält, wählen Sie entweder die URL der RA aus, die die ursprüngliche Zertifikatsanforderung genehmigt hat, oder geben Sie die URL in das Textfenster ein. Wenn Sie die URL nicht kennen, setzen Sie sich mit dem Administrator der Registrierungsdomäne in Verbindung.

Begründung für den Widerruf
Wählen Sie einen der folgenden Einträge aus, um den Grund für den Widerruf des Zertifikats anzugeben.

- **Der Benutzerschlüssel war beschädigt**
- **Der CA-Schlüssel war beschädigt**
- **Benutzer hat die Zugehörigkeit geändert**

- **Das Zertifikat wurde ersetzt**
- **Der ursprüngliche Verwendungszweck des Zertifikats ist nicht mehr gültig**
- **Zertifikat in den Wartestatus setzen**
- **Das Zertifikat wird nicht mehr verwendet**

Im Abschnitt „Begründung für den Widerruf von Zertifikaten" auf Seite 37 werden diese Begründungen definiert.

Dialog 'Datei unterzeichnen'

In diesem Dialog können Sie ein Zertifikat verwenden, um eine Datei zu unterzeichnen. Wenn Sie eine Datei mit einer digitalen Unterschrift unterzeichnen, kann jeder, der die Datei öffnet, erkennen, ob der Inhalt der Datei seit der Unterzeichnung geändert wurde.

Eingabedatei
Geben Sie den Pfad und den Namen der Datei an, die Sie unterzeichnen wollen. Über den Knopf **Durchsuchen** können Sie den Pfad und Dateinamen auswählen, anstatt diese Angaben manuell einzugeben.

Ausgabedatei
Geben Sie den Pfad und den Namen für die Datei nach deren Unterzeichnung an. Über den Knopf **Durchsuchen** können Sie den Pfad und Dateinamen auswählen, anstatt diese Angaben manuell einzugeben.

Unterschriftsalgorithmus
Wählen Sie den Algorithmus aus, den Sie zur Unterzeichnung der Datei verwenden wollen.

SHA1 With RSA
Generiert eine Unterschrift, indem ein sicherer Hash-Algorithmus (SHA-1) auf die im RSA-Standard (Rivest, Shamir und Adleman) definierte Unterschriftenberechnung angewandt wird. Mit RSA erfolgt die Überprüfung der Unterschrift relativ schnell. Allerdings dauert die Erstellung der Unterschrift unter Umständen länger als bei anderen Algorithmen.

MD5 With RSA
Generiert eine Unterschrift, indem die Nachrichtenauszugsfunktion MD5 auf die im RSA-Standard definierte Unterschriftenberechnung angewandt wird. Der MD5-Algorithmus ist schneller als SHA-1. Allerdings erstellt SHA-1 einen größeren Nachrichtenauszug, so daß es möglicherweise schwieriger ist, diese Unterschrift unbefugt zu manipulieren.

Wenn Sie Dateien vor dem Unterzeichnen anzeigen wollen, klicken Sie auf **Anzeigen**. Mit dieser Aktion wird die Anwendung aufgerufen, die dem Dateityp der unterzeichneten Datei zugeordnet ist.

Dialog 'Smart Card-Eigenschaften'

In diesem Dialog können Sie die Informationen zu der geöffneten Smart Card überprüfen.

Smart Card
Der Name der Smart Card.

PKCS #11-Version
Die Stufe der PKCS #11-Verschlüsselung.

CDSA-Version

Die Stufe der CDSA (Common Data Security Architecture, Sicherheitsarchitektur für Basisdaten), die die Smart Card während der Verschlüsselung und Datenspeicherung verwendet. Sie können diese Smart Card nicht mit einer Smart Card-Software verwenden, die eine ältere als die aufgeführte CDSA-Version unterstützt.

Verfügbarer Speicherplatz auf der Smart Card

Der verbleibende Speicherplatz zum Sichern von Zertifikaten und Zertifikatsanforderungen.

Hilfe für die Client-Anwendung

Die Client-Anwendung stellt folgende Hilfefunktionen zur Verfügung:

- Das Fenster 'Smart Card' verfügt über das Menü **Hilfe** mit den folgenden Optionen:

  Hilfethemen

  Zeigt das *Benutzerhandbuch von Trust Authority* an.

  Zu diesem Fenster

  Zeigt einen Hilfetext für das aktuelle Fenster an.
- Jeder Dialog verfügt über den Knopf **Hilfe**, mit dem Sie einen Hilfetext zu der von Ihnen jeweils ausgeführten Task anzeigen können.
- Jedes Feld verfügt über einen kontextbezogenen Hilfetext, der angezeigt wird, wenn der Cursor sich in dem entsprechenden Feld befindet.

Zugehörige Abschnitte:

„Zwischen Registerkarten wechseln" auf Seite 22

Überlegungen zur Unterstützung in der Landessprache

In diesem Abschnitt werden die Unterschiede zusammengefaßt, die zwischen der englischen Version von Trust Authority und den Versionen in anderen unterstützten Sprachen bestehen. Wenn Sie Zertifikate anfordern oder verwalten, die eine nicht-englische Trust Authority-Version verwenden, lesen Sie diesen Abschnitt, um zu erfahren, welche Unterschiede es beim Anzeigen und Verarbeiten von Daten in Ihrer jeweiligen Sprache möglicherweise gibt.

Es folgt eine Liste der Sprachencodes für die unterstützten Sprachen:

- `de_DE` für Deutsch
- `en_US` für Englisch
- `es_ES` für Spanisch
- `fr_FR` für Französisch
- `it_IT` für Italienisch
- `ja_JP` für Japanisch
- `ko_KR` für Koreanisch
- `pt_BR` für brasilianisches Portugiesisch
- `zh_CN` für vereinfachtes Chinesisch
- `zh_TW` für traditionelles Chinesisch

Zertifikate mit Nicht-ASCII-DNs anfordern

Sie können Trust Authority dazu verwenden, Zertifikate mit Nicht-ASCII-DNs (Distinguished Names = registrierte Namen) anzufordern, wie beispielsweise Zertifikate, in denen für den allgemeinen Namen Zeichen in der für die jeweilige Landessprache spezifischen Schreibweise verwendet

werden. Die DNs der von Trust Authority erstellten Zertifikate werden in druckbaren Zeichen, Teletex (T.61)- oder UTF-8-Zeichen codiert. Normalerweise werden DNs, die Zeichen in der für europäische Landessprachen spezifischen Schreibweise enthalten, in Teletex codiert und DNs, die Zeichen in der für Chinesisch, Japanisch oder Koreanisch spezifischen Schreibweise enthalten, in UTF-8. Je nach Browser-Typ und dessen jeweiliger Lokalisierung für Ihre Umgebung werden diese Zertifikate möglicherweise nicht korrekt angezeigt.

Netscape für Zertifikate mit Nicht-ASCII-DNs verwenden

Netscape-Browser können Zertifikate, die mit UTF-8 codiert sind, nicht verarbeiten. Trust Authority codiert DNs, die Doppelbytezeichen enthalten (in Chinesisch, Japanisch oder Koreanisch) mit UTF-8. Da die derzeit verfügbaren Versionen von Netscape die mit UTF-8 codierten Zertifikate nicht verarbeiten können, kann Netscape nicht zum Anforderung oder Importieren von Zertifikaten verwendet werden, deren DNs Zeichen in chinesischer, japanischer oder koreanischer Landesspreche enthalten. Verwenden Sie statt dessen Microsoft Internet Explorer zum Anfordern von Zertifikaten in diesen Landessprachen.

Netscape zum Anzeigen der Schlüsselgröße verwenden

Bei der Verwendung von Netscape mit einer nicht-englischen Version des Browser-Registrierungsformulars wird unleserlicher Text im Feld für die Schlüsselgröße in Kästchen ([][][]) angezeigt. Dieser Text wird intern vom Browser generiert und weist kein UTF-8-Format auf. Der Netscape-Browser generiert diese Textzeichenfolge ausschließlich in den Basiszeichensätzen (wie beispielsweise ISO-8859-1 für Englisch und westeuropäische Landessprachen, Big5 für traditionelles Chinesisch und BG2312 für vereinfachtes Chinesisch).

Da die JSP-Registrierungsseiten in UTF-8 codiert sind, erkennt der Browser die Zeichenfolge im Basiszeichensatz nicht. Daher kann diese Zeichenfolge im Browser nicht mit dem UTF-8-Zeichensatz angezeigt werden.

Die Auswahlmöglichkeiten für die Schlüsselgröße in einer US-Version des Netscape-Browsers lauten wie folgt:

- 1024 (High Grade)
- 768 (Medium Grade)
- 512 (Low Grade)

Aufgrund von Exporteinschränkungen durch die US-Regierung enthält die Liste für eine nicht-englische Version des Browsers wahrscheinlich nur einen Eintrag mit einer 512-Bit-Schlüsselgröße (Low Grade).

Auf Client-Anwendungsnachrichtendateien zugreifen

Nach der Installation der Trust Authority-Client-Anwendung muß die Umgebungsvariable NLSPATH wie folgt aktualisiert werden:

```
Von:  C:\Progra~1\IBM\TrustA~1\msg\%L\%N
  In:  C:\Progra~1\IBM\TrustA~1\TACLIENT\msg\%L\%N
```

Diese Änderung ermöglicht das Anzeigen von Fehlernachrichten in der korrekten Sprache.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme und Dienstleistungen in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Änderung des Textes bleibt vorbehalten.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne daß eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäfts-

bedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Garantie, daß diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen. Diese Daten stellen deshalb keine Leistungsgarantie dar.

Informationen über Produkte anderer Hersteller als IBM wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröffentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat diese Produkte nicht getestet und übernimmt im Hinblick auf Produkte anderer Hersteller keine Verantwortung für einwandfreie Funktion, Kompatibilität oder andere Ansprüche. Fragen hinsichtlich des Leistungsspektrums von Produkten anderer Hersteller als IBM sind an den jeweiligen Hersteller des Produkts zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Marken und Dienstleistungsmarken

Folgende Namen sind in gewissen Ländern Marken der IBM Corporation:

IBM
AIX
AIX/6000
DB2
DB2 Universal Database
SecureWay
WebSphere

Das Programm Trust Authority (im folgenden als "Programm" bezeichnet) enthält Komponenten von DB2 Universal Database. Diese Komponenten dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden, um Daten zu speichern und zu verwalten, die vom Programm verwendet oder generiert werden. Für andere Datenverwaltungsoperationen ist der Einsatz nicht gestattet. Diese Lizenz gilt z. B. nicht für eingehende Verbindungen zur Datenbank, die von anderen Anwendungen aus für Abfragen und Berichtserstellungsoperationen hergestellt werden. Sie sind lediglich zur Installation und Verwendung dieser Komponenten auf der gleichen Maschine berechtigt, auf der auch das Programm installiert und verwendet wird.

Das Programm enthält Komponenten des IBM WebSphere Application Server und des IBM HTTP Web Server ("IBM Server"). Sie sind nicht berechtigt, die IBM Server zu anderen Zwecken als in Verbindung mit der lizenzgerechten Verwendung des Programms zu benutzen. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Java und alle auf Java basierenden Marken und Logos sind in gewissen Ländern Marken der Sun Microsystems, Inc.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Pentium ist in gewissen Ländern eine Marke der Intel Corporation.

Dieses Programm enthält Sicherheitssoftware von RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. Alle Rechte vorbehalten.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Hewlett-Packard Company. Copyright (c) 1994.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Hewlett-Packard Company macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Silicon Graphics Computer Systems, Inc. Copyright (c) 1996 - 1999.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Silicon Graphics macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken anderer Unternehmen sein.

Bezugsinformationen

Die Trust Authority-Produktdokumentation steht auf der CD-ROM *IBM SecureWay Trust Authority-Dokumentation* im PDF-Format (Portable Document Format) und im HTML-Format zur Verfügung. Die HTML-Versionen einiger Veröffentlichungen sind mit dem Produkt installiert und können über die Benutzerschnittstelle abgerufen werden.

Bitte beachten Sie, daß das Produkt seit Erstellung der Veröffentlichungen möglicherweise geändert worden ist. Aktuelle Produktinformationen sowie Informationen für den Zugriff auf Veröffentlichungen in der Sprache und im Format Ihrer Wahl finden Sie in der Informationsdatei *Readme*. Die neueste Version der *Readme*-Datei steht auf der folgenden Web-Site von IBM SecureWay Trust Authority zur Verfügung:

`http://www.tivoli.com/support`

Zur Trust Authority-Bibliothek gehört die folgende Dokumentation:

Einführung
: Dieses Buch bietet eine Übersicht über das Produkt. Es enthält die Produktvoraussetzungen, beschreibt die Installationsverfahren und stellt Informationen darüber zur Verfügung, wie Sie auf die Online-Hilfefunktion für die jeweiligen Produktkomponenten zugreifen können. Dieses Buch liegt in gedruckter Form vor und wird mit dem Produkt geliefert.

Systemverwaltung
: Dieses Buch bietet allgemeine Informationen zur Verwaltung des Trust Authority-Systems. Es beschreibt die Prozeduren zum Starten und Stoppen der Server, zum Ändern von Kennwörtern, zur Verwaltung der Server-Komponenten sowie zum Erstellen von Protokollen und zur Ausführung von Datenintegritätsüberprüfungen.

Konfiguration
: Dieses Buch enthält Informationen darüber, wie ein Trust Authority-System mit Hilfe des Konfigurationsassistenten (Setup Wizard) konfiguriert wird. Während Sie die Online-Hilfefunktion für den Assistenten anzeigen, können Sie auf die HTML-Version dieses Handbuchs zugreifen.

RA Desktop
: Dieses Buch enthält Informationen darüber, wie Zertifikate im gesamten Zertifikatsverarbeitungszyklus mit Hilfe von RA Desktop verwaltet werden. Während Sie die Online-Hilfefunktion für den Desktop anzeigen, können Sie auf die HTML-Version dieses Handbuchs zugreifen.

Benutzerhandbuch
: Dieses Buch enthält Informationen darüber, wie Zertifikate abgerufen und verwaltet werden. Es beschreibt die Prozeduren zur Verwendung der Browser-Registrierungsformulare von Trust Authority, um Zertifikate anzufordern, zu erneuern und zu widerrufen. Außerdem beschreibt das Buch, wie eine Vorabregistrierung für PKIX-kompatible Zertifikate durchgeführt wird und wie diese Zertifikate mit Hilfe des Trust Authority Client verwaltet werden. Während Sie die Online-Hilfefunktion für den Client anzeigen, können Sie auf die HTML-Version dieses Handbuchs zugreifen.

Anpassung

Dieses Buch zeigt, wie die Trust Authority-Registrierungsfunktion angepaßt wird, um die Vorgaben zur Registrierung und Zertifizierung im Rahmen Ihrer Unternehmensregeln zu unterstützen. Sie erfahren beispielsweise, wie HTML- und Java Server-Seiten, Mitteilungsschreiben, Zertifikatsprofile und Regel-Exits angepaßt werden.

Die Trust Authority-Website enthält weitere Dokumente, die Ihnen bei der Installation, Verwaltung un Nutzung von Trust Authority helfen können. Dort finden Sie beispielsweise zusätzliche Richtlinien zum Directory-Schema und erfahren, wie Trust Authority in den IBM SecureWay 4758 PCI Cryptographic Coprocessor integriert wird.

Glossar

In diesem Glossar werden alle Termini und Abkürzungen definiert, die in diesem Handbuch verwendet werden und die möglicherweise neu oder unbekannt und von Bedeutung sind.

Numerische Einträge

4758 PCI Cryptographic Coprocessor. Eine programmierbare, manipulationssensitive PCI-Bus-Verschlüsselungskarte, die die Ausführung von DES- und RSA-Verschlüsselungsoperationen mit hoher Geschwindigkeit ermöglicht. Die Verschlüsselungsprozesse werden in einem gesicherten und abgegrenzten Bereich auf der Karte ausgeführt. Die Karte entspricht den strengen Anforderungen des FIPS PUB 140-1 Level 4-Standards. In dem gesicherten und abgegrenzten Bereich kann Software ausgeführt werden. Der SET-Standard kann z. B. zur Verarbeitung von Kreditkartentransaktionen genutzt werden.

A

Abstract Syntax Notation One (ASN.1). Eine ITU-Notation, die zum Definieren der Syntax von Informationsdaten benutzt wird. Sie definiert eine Reihe einfacher Datentypen und gibt eine Notation für die Identifizierung dieser Typen und die Angabe von Werten für diese Typen an. Diese Notationen können verwendet werden, wenn es erforderlich ist, die abstrakte Syntax von Informationen zu definieren, ohne damit die Art der Verschlüsselung dieser Informationen für die Übertragung zu beeinträchtigen.

ACL. Access Control List - Zugriffssteuerungsliste.

Aktionsprotokoll. Die Aufzeichnung aller Ereignisse, die während der gesamten Gültigkeitsdauer eines Identitätsnachweises aufgetreten sind.

American National Standard Code for Information Interchange (ASCII). Der Standardcode, der für den Austausch von Informationen zwischen Datenverarbeitungssystemen, DFV-Systemen und zugehöriger Hardware verwendet wird. ASCII verwendet einen codierten Zeichensatz, der aus Zeichen von 7 Bit Länge (bzw. 8 Bit bei Paritätsprüfung) besteht. Der Zeichensatz besteht hierbei aus Steuerzeichen und Schriftzeichen.

American National Standards Institute (ANSI). Eine Organisation, die die Verfahrensweisen definiert, mit deren Hilfe akkreditierte Organisationen freiwillig eingehaltene Industriestandards in den Vereinigten Staaten festlegen und verwalten. Ihr gehören Hersteller, Verbraucher und allgemeine Interessenvertretungen an.

Anforderungs-ID. Ein aus 24 bis 32 Zeichen bestehender ASCII-Wert, der zur eindeutigen Identifikation einer Zertifikatsanforderung gegenüber der RA dient. Dieser Wert kann bei der Transaktion für die Zertifikatsanforderung verwendet werden, um den Status der Anforderung oder des zugehörigen Zertifikats abzurufen.

ANSI. American National Standards Institute.

Applet. Ein in der Programmiersprache Java geschriebenes Computerprogramm, das innerhalb eines Java-kompatiblen Web-Browsers ausgeführt werden kann. Dieses wird auch als Java-Applet bezeichnet.

Art. *Siehe* Objektart.

ASCII. American National Standard Code for Information Interchange.

ASN.1. Abstract Syntax Notation One.

Asymmetrische Verschlüsselung. Ein Verschlüsselungsverfahren, das zur Ver- und Entschlüsselung unterschiedliche, asymmetrische Schlüssel verwendet. Jedem Benutzer wird hierbei ein Schlüsselpaar zugeordnet, das einen allgemeinen, für alle zugänglichen Schlüssel und einen privaten Schlüssel umfaßt, der nur dem jeweiligen Benutzer bekannt ist. Eine gesicherte Transaktion kann ausgeführt werden, wenn der öffentliche Schlüssel sowie der zugehörige private Schlüssel übereinstimmen. In diesem Fall kann die Transaktion entschlüsselt werden. Dieses Verfahren wird auch als Verschlüsselung auf der Basis von Schlüsselpaaren bezeichnet. *Gegensatz zu* Symmetrische Verschlüsselung.

Asynchrone Übertragung. Ein Übertragungsmodus, bei dem Sender und Empfänger nicht gleichzeitig vorhanden sein müssen.

Authentifizierung. Der Vorgang, bei dem die Identität eines Teilnehmers an einer Übertragung zuverlässig überprüft wird.

B

Base64-Verschlüsselung. Ein häufig verwendetes Verfahren bei der Übertragung von Binärdaten mit MIME.

Basic Encoding Rules (BER). Die Regeln, die in ISO 8825 für die Verschlüsselung von in ASN.1 beschriebenen Dateneinheiten angegeben sind. Die Regeln geben das Verschlüsselungsverfahren, jedoch nicht die abstrakte Syntax an.

Benutzerauthentifizierung. Der Prozeß, mit dem überprüft wird, ob der Absender einer Nachricht die berechtigte Person ist, als die er sich ausgibt. Der Prozeß überprüft außerdem, ob ein Kommunikationsteilnehmer auch tatsächlich mit dem erwarteten Endbenutzer oder System in Verbindung steht.

BER. Basic Encoding Rules.

Berechtigung. Die Erlaubnis, auf eine Ressource zuzugreifen.

Bestreiten. Etwas als unwahr zurückweisen. Dies ist z. B. dann der Fall, wenn ein Benutzer abstreitet, eine bestimmte Nachricht gesendet oder eine bestimmte Anforderung übergeben zu haben.

Browser. *Siehe* Web-Browser.

Browser-Zertifikat. Ein digitales Zertifikat, das auch als Zertifikat der Client-Seite bezeichnet wird. Es wird von einem CA über einen für SSL aktivierten Web-Server ausgestellt. Die Schlüssel in einer verschlüsselten Datei ermöglichen dem Inhaber des Zertifikats das Verschlüsseln, Entschlüsseln und Unterzeichnen von Daten. Normalerweise werden diese Schlüssel im Web-Browser gespeichert. In bestimmten Anwendungen können die Schlüssel auf Smart-Cards oder anderen Speichermedien gespeichert werden. *Siehe auch* Digitales Zertifikat.

Bytecode. Maschinenunabhängiger Code, der mit dem Java-Compiler generiert und mit dem Java-Interpreter ausgeführt wird.

C

CA. Certificate Authority - Zertifikatsaussteller.

CA-Hierarchie. Bei Trust Authority eine Sicherungsstruktur, bei der ein CA auf der höchsten Ebene positioniert ist. Anschließend können bis zu vier weitere Ebenen mit untergeordneten CAs definiert werden. Wenn Benutzer oder Server bei einem Zertifikatsaussteller registriert werden, wird ihnen ein von diesem Aussteller unterzeichnetes Zertifikat zugeordnet. Außerdem übernehmen sie die Zertifizierungshierarchie der übergeordneten Ebenen.

CA-Server. Der Server für die CA-Komponente von Trust Authority.

CA-Zertifikat. Ein Zertifikat, das vom Web-Browser eines Benutzers auf dessen Anforderung hin von einem nicht identifizierten CA akzeptiert wird. Der Browser kann dann dieses Zertifikat verwenden, um für die Kommunikation mit Servern, die über Zertifikate dieses CAs verfügen, eine Authentifizierung durchzuführen.

CAST-64. Ein Block-Cipher-Algorithmus, der mit einer Blockgröße von 64 Bit und einem 6-Bit-Schlüssel arbeitet. Er wurde von Carlisle Adams und Stafford Tavares entwickelt.

CCA. Common Cryptographic Architecture.

CDSA. Common Data Security Architecture.

CGI. Common Gateway Interface.

Client. (1) Eine Funktionseinheit, die gemeinsam benutzte Services von einem Server empfängt. (2) Ein Computer oder Programm, der/das Services von einem anderen Computer oder Programm anfordert.

Client/Server. Ein Modell für die verteilte Verarbeitung, bei dem ein Programm an einem Standort eine Anforderung an ein Programm an einem anderen Standort sendet und auf eine Antwort wartet. Das anfordernde Programm wird als Client, das antwortende als Server bezeichnet.

Codeunterzeichnung. Ein Verfahren zum Unterzeichnen ausführbarer Programme mit einer digitalen Unterschrift. Die Codeunterzeichnung dient zur Verbesserung der Zuverlässigkeit von Softwarekomponenten, die über das Internet verteilt werden.

Common Cryptographic Architecture (CCA). IBM Software, die einen konsistenten Verschlüsselungsansatz auf den wichtigsten IBM Computerplattformen bietet. Sie unterstützt Anwendungssoftware, die in einer Vielzahl von Programmiersprachen geschrieben wurde. Die Anwendungssoftware kann hierbei die CCA-Services aufrufen, um eine breite Palette kryptografischer Funktionen (einschließlich der DES- und der RSA-Verschlüsselung) auszuführen.

Common Data Security Architecture (CDSA). Eine Initiative zum Definieren eines umfassenden Ansatzes für Sicherheitsservices und Sicherheitsverwaltungsoperationen bei computerbasierten Sicherheitsanwendungen. Diese Architektur wurde von Intel entworfen und dient dazu, Computerplattformen für Anwendungen sicherer zu gestalten.

Common Gateway Interface (CGI). Ein Standardverfahren zum Übertragen von Informationen zwischen Web-Seiten und Web-Servern.

CRL. Certificate Revocation List - Zertifikatswiderrufsliste.

CRL-Veröffentlichungsintervall. Dieses Intervall wird in der CA-Konfigurationsdatei definiert und gibt das Zeitintervall zwischen zwei Veröffentlichungen der Zertifikatswiderrufsliste im Directory an.

D

Dämon. Ein Programm, das Tasks im Hintergrund ausführt. Es wird implizit aufgerufen, wenn eine Bedin-

gung auftritt, die die Hilfe des Dämons erforderlich macht. Es ist nicht erforderlich, daß der Benutzer über die Ausführung des Dämons unterrichtet wird, da der Dämon normalerweise vom System automatisch gestartet wird. Ein Dämon kann über eine unbegrenzte Zeit hinweg ausgeführt oder vom System in bestimmten Zeitintervallen erneut generiert werden.

Der Terminus (englisch *demon*) stammt aus der Mythologie. Später wurde er aber als Akronym für den Ausdruck "Disk And Execution MONitor" (Platten- und Ausführungsüberwachungsprogramm) erklärt.

Data Encryption Standard (DES). Eine Verschlüsselungs-Block-Cipher, die 1977 von der US-Regierung als offizieller Standard definiert und übernommen wurde. Dieser Standard wurde ursprünglich von IBM entwickelt. DES wurde seit seiner Veröffentlichung umfassend untersucht und stellt ein allgemein bekanntes und häufig verwendetes Verschlüsselungssystem zur Verfügung.

Bei DES handelt es sich um ein symmetrisches Verschlüsselungssystem. Um es für die Datenübertragung einzusetzen, müssen sowohl der Sender als auch der Empfänger den selben, geheimen Schlüssel kennen. Dieser Schlüssel wird zum Ver- und Entschlüsseln der Nachricht verwendet. DES kann außerdem zur Durchführung von Verschlüsselungsoperationen für einzelne Benutzer eingesetzt werden, z. B. zum Speichern von verschlüsselten Dateien auf einer Festplatte. DES arbeitet mit einer Blockgröße von 64 Bit und verwendet für die Verschlüsselung einen 56-Bit-Schlüssel. Ursprünglich wurde dieser Standard für die Hardwareimplementierung entwickelt. DES wird von NIST alle fünf Jahre erneut als offizieller Verschlüsselungsstandard der US-Regierung zertifiziert.

Datenspeicherbibliothek (DL). Ein Modul, das den Zugriff auf permanente Datenspeicher mit Zertifikaten, CRLs, Schlüsseln, Regeln und anderen sicherheitsrelevanten Objekten ermöglicht.

DEK. Document Encryption Key = Dokumentverschlüsselungsschlüssel.

DER. Distinguished Encoding Rules.

DES. Data Encryption Standard.

Diffie-Hellman. Ein Verfahren zur Datenverschlüsselung, das auf der Verwendung eines gemeinsamen Schlüssels auf einem nicht gesicherten Medium basiert und nach seinen Erfindern (Whitfield Diffie und Martin Hellman) benannt wurde.

Digital Signature Algorithm (DSA). Ein auf öffentlichen Schlüsseln basierender Algorithmus, der zum Standard für digitale Unterschriften (Digital Signature Standard = DSS) gehört. Er kann nur für digitale Unterschriften, jedoch nicht für die Verschlüsselung verwendet werden.

Digitale Unterschrift. Eine codierte Nachricht, die an Dokumente oder Daten angefügt wird, und die Identität des Absenders nachweist.

Eine digitale Unterschrift gewährleistet ein höheres Maß an Sicherheit als eine physische Unterschrift, da es sich hierbei nicht lediglich um einen verschlüsselten Namen oder eine Reihe einfacher Identifikationscodes handelt. Eine digitale Unterschrift enthält eine verschlüsselte Zusammenfassung der unterzeichneten Nachricht. Durch das Anfügen einer digitalen Unterschrift an eine Nachricht läßt sich der Absender also zweifelsfrei feststellen. (Die Unterschrift kann nur mit Hilfe des Schlüssels des Absenders erstellt werden.) Außerdem ermöglicht sie die Absicherung des Inhalts der unterzeichneten Nachricht, da die verschlüsselte Nachrichtenzusammenfassung mit dem Nachrichteninhalt übereinstimmen muß. Andernfalls wird die Unterschrift nicht als gültig identifiziert. Eine digitale Unterschrift kann also nicht von einer Nachricht kopiert und für eine andere Nachricht verwendet werden, da sonst die Zusammenfassung (Hash-Code) nicht übereinstimmen würde. Alle Änderungen an der unterzeichneten Nachricht führen automatisch zum Verlust der Gültigkeit der Unterschrift.

Digitale Zertifizierung. *Siehe* Zertifizierung.

Digitales Zertifikat. Ein elektronischer Identitätsnachweis, der von einer zuverlässigen Stelle für eine Person oder Entität ausgestellt wird. Jedes Zertifikat ist mit dem privaten Schlüssel des CAs unterzeichnet. Es bürgt für die Identität einer Person, eines Unternehmens oder einer Organisation.

Abhängig vom Aufgabenbereich des CAs kann das Zertifikat die Berechtigung seines Inhabers bestätigen, e-Business-Transaktionen über das Internet auszuführen. In gewisser Weise hat ein digitales Zertifikat eine ähnliche Funktion wie ein Führerschein oder ein Meisterbrief. Es bestätigt, daß der Inhaber des entsprechenden privaten Schlüssels berechtigt ist, bestimmte e-Business-Aktivitäten auszuführen.

Ein Zertifikat enthält Informationen über die Entität, die von ihm zertifiziert wird, gibt an, ob es sich um eine Person, eine Maschine oder ein Computerprogramm handelt und enthält als Teil dieser Informationen den zertifizierten öffentlichen Schlüssel dieser Entität.

Directory. Eine hierarchische Struktur, die als globales Repository für Informationen zur Datenkommunikation (wie beispielsweise E-Mail oder Austausch von verschlüsselten Daten) konzipiert ist. Im Directory werden bestimmte Elemente gespeichert, die für die PKI-Struktur (PKI = Public Key Infrastructure) unbedingt erforderlich sind. Hierzu gehören die folgenden Elemente: öffentliche Schlüssel, Zertifikate und Zertifikatswiderrufslisten (CRLs).

Die Daten im Directory sind hierarchisch in einer Baumstruktur organisiert, wobei die oberste Ebene der Baumstruktur das Root-Verzeichnis ist. Häufig stehen

Organisationen einer höheren Ebene für einzelne Länder, Regierungen oder Unternehmen. Benutzer oder Einheiten werden im allgemeinen als ″Blätter″ einer solchen Baumstruktur dargestellt. Diese Benutzer, Organisationen, Standorte, Länder und Einheiten haben jeweils ihren eigenen Eintrag. Jeder Eintrag besteht aus Attributen, denen verschiedene Typen zugewiesen sind. Diese enthalten Informationen zu den Objekten, für die der jeweilige Eintrag steht.

Jeder Eintrag im Directory ist mit einem zugeordneten registrierten Namen (DN = Distinguished Name) verbunden. Dieser ist eindeutig, wenn der Eintrag ein Attribut umfaßt, das für das tatsächliche Objekt als eindeutig bekannt ist. Im folgenden DN-Beispiel wurde als Land (C = Country) US, als Unternehmen (O = Organization) IBM, als Unternehmenseinheit (OU = Organization Unit) Trust und als allgemeiner Name (CN = Common Name) der Wert CA1 angegeben.

```
C=US/O=IBM/OU=Trust/CN=CA1
```

Directory-Server. Unter Trust Authority das IBM SecureWay Directory. Dieses Directory unterstützt die LDAP-Standards und verwendet DB2 als Basissystem.

Distinguished Encoding Rules (DER). Durch DER werden bestimmte Einschränkungen für BER definiert. Mit DER kann genau ein bestimmter Verschlüsselungstyp aus den verfügbaren und auf der Basis der Verschlüsselungsregeln als zulässig definierten Typen ausgewählt werden. Hierdurch werden alle Senderoptionen eliminiert.

DL. Data Storage Library = Datenspeicherbibliothek.

DN. Distinguished Name - Registrierter Name.

Dokumentverschlüsselungsschlüssel (DEK). Normalerweise ein symmetrischer Ver-/Entschlüsselungsschlüssel, z. B. DES.

Domäne. *Siehe* Sicherheitsdomäne *und* Registrierungsdomäne.

DSA. Digital Signature Algorithm.

E

e-Business. Das Durchführen geschäftlicher Transaktionen über Netze und Computer, z. B. der Kauf und Verkauf von Waren und Dienstleistungen sowie der Transfer von Zahlungsmitteln mit Hilfe der digitalen Kommunikation.

e-Commerce. Unternehmensübergreifende Transaktionen wie beispielsweise der Kauf und Verkauf von Waren und Dienstleistungen (zwischen Unternehmen und ihren Kunden, Lieferanten, Subunternehmen und anderen) über das Internet. E-Commerce stellt einen Kernbestandteil des e-Business dar.

Endentität. Der Gegenstand eines Zertifikats, bei dem es sich nicht um einen CA handelt.

Entschlüsseln. Den Verschlüsselungsprozeß rückgängig machen.

Exemplar. Bei DB2 bezeichnet man als Exemplar eine logische Datenbankverwaltungsumgebung zum Speichern von Daten und Ausführen von Anwendungen. Es ermöglicht die Definition einer allgemeinen Gruppe von Konfigurationsparametern für verschiedene Datenbanken.

Extranet. Ein Netz, das auf dem Internet basiert und eine ähnliche Technologie einsetzt. Unternehmen beginnen momentan mit dem Einsatz des Web Publishings, elektronischen Handels und der Nachrichtenübertragung sowie der Verwendung von Groupware für verschiedene Gruppen von Kunden, Partnern und internen Mitarbeitern.

F

File Transfer Protocol (FTP). Ein Client/Server-Protokoll im Internet, das zum Übertragen von Dateien zwischen Computern benutzt wird.

Firewall. Ein Gateway zwischen Netzen, der den Informationsfluß zwischen diesen einschränkt. Normalerweise dienen Firewalls dem Schutz interner Netze gegen die nicht berechtigte Verwendung durch externe Personen.

FTP. File Transfer Protocol.

G

Gateway. Eine Funktionseinheit, mit deren Hilfe nicht kompatible Netze oder Anwendungen Daten austauschen können.

Gegenseitige Zertifizierung. Ein Trust-Modell, bei dem ein CA für einen anderen CA ein Zertifikat ausstellt, das den öffentlichen Schlüssel enthält, der dem entsprechenden privaten Unterschriftsschlüssel zugeordnet ist. Ein gegenseitig zertifiziertes Zertifikat ermöglicht Client-Systemen oder Endentitäten in einer Verwaltungsdomäne die sichere Kommunikation mit Client-Systemen oder Endentitäten in einer anderen Domäne.

Gesicherte Computerbasis (TCB). Die Software- und Hardwareelemente, die zur Umsetzung der Computersicherheitsregeln eines Unternehmens verwendet werden. Alle Elemente oder Teilelemente, die zur Implementierung der Sicherheitsregeln eingesetzt werden können, sind sicherheitsrelevant und Bestandteil der TCB. Bei der TCB handelt es sich um ein Objekt, das durch die Sicherheitsperipherie begrenzt wird. Die Mechanismen, die zur praktischen Umsetzung der Sicherheitsregeln eingesetzt werden, dürfen nicht umgangen werden können und müssen verhindern, daß Programme Zugriff auf Systemprivilegien erlangen können, für die sie nicht berechtigt sind.

H

Höchster CA. Der CA, der innerhalb der PKI-CA-Hierarchie die höchste Position einnimmt.

HTML. Hypertext Markup Language.

HTTP. Hypertext Transaction Protocol.

HTTP-Server. Ein Server, der die Web-gestützte Kommunikation mit Browsern und anderen Programmen im Netz steuert.

Hypertext. Textsegmente, die einzelne oder mehrere Wörter umfassen oder Bilder enthalten, auf die der Leser mit der Maus klicken kann, um ein anderes Dokument aufzurufen und anzuzeigen. Diese Textsegmente werden als Hyperlinks bezeichnet. Ruft der Leser diese anderen Dokumente auf, stellt er zu diesen eine Hyperlink-Verbindung her.

Hypertext Markup Language (HTML). Eine Formatierungssprache für das Codieren von Web-Seiten. HTML basiert auf SGML (Standard Generalized Markup Language).

Hypertext Transaction Protocol (HTTP). Ein Client/Server-Protokoll für das Internet, mit dem Hypertext-Dateien im Web übertragen werden.

I

ICL. Issued Certificate List - Liste der ausgestellten Zertifikate.

Identitätsnachweis. Vertrauliche Informationen, die verwendet werden, um beim Austausch von Daten während der Authentifizierung die eigene Identität zu belegen. In Network Computing-Umgebungen ist die am häufigsten verwendete Form des Identitätsnachweises ein Zertifikat, das von einem CA erstellt und unterzeichnet wurde.

IniEditor. Bei Trust Authority ein Tool, mit dem Konfigurationsdateien editiert werden können.

Integrität. Ein System schützt seine Datenintegrität, wenn es die Änderung dieser Daten durch nicht berechtigte Personen verhindert. (Im Gegensatz hierzu versteht man unter dem Schutz der Vertraulichkeit von Daten, wenn verhindert wird, daß diese unberechtigten Personen zugänglich gemacht werden.)

Integritätsprüfung. Die Prüfung der Protokolleinträge, die für Transaktionen mit externen Komponenten aufgezeichnet wurden.

International Standards Organization (ISO). Eine internationale Organisation, die Standards für eine breite Palette von Industriebereichen, z. B. auch für Computernetzprotokolle, entwickelt und veröffentlicht.

International Telecommunication Union (ITU). Eine internationale Organisation, in der Verwaltungs- und private Industriebereiche globale Datenfernübertragungsnetze und -services koordinieren. Bei der Veröffentlichung von Informationen zur Datenfernübertragungstechnologie sowie den entsprechenden Regelwerken und Standards nimmt sie eine führende Position ein.

Interne Struktur. *Siehe* Schema.

Internet. Ein weltweiter Verbund von Netzen, die die elektronische Verbindung zwischen Computern und die Kommunikation zwischen den Computern über Softwareeinrichtungen wie elektronische Post (E-Mail) oder Web-Browser ermöglichen. So sind beispielsweise die meisten Universitäten in ein Netz eingebunden, das seinerseits eine Verbindung zu anderen ähnlichen Netzen hat, die zusammen das Internet bilden.

Internet Engineering Task Force (IETF). Eine Gruppe, die sich schwerpunktmäßig mit dem Entwickeln und Definieren von Protokollen für das Internet befaßt. Sie repräsentiert eine internationale Gruppe von Netzdesignern, -bedienern, -herstellern und -forschern. Die Aufgabe der IETF ist die Entwicklung der Internet-Architektur sowie die Gewährleistung der reibungslosen Verwendung des Internets.

Intranet. Ein Netz innerhalb eines Unternehmens, das sich im allgemeinen hinter Firewalls befindet. Es basiert auf dem Internet und setzt eine ähnliche Technologie ein. Vom technischen Standpunkt aus ist ein Intranet eine Erweiterung des Internets. Zu den in beiden Netzen benutzten Komponenten gehören z. B. HTML und HTTP.

IPSec. Ein von der IETF entwickelter IPS-Standard (IPS = Internet Protocol Security). IPSec ist ein Protokoll der Vermittlungsschicht, das entwickelt wurde, um Services für die Gewährleistung der Sicherheit bei der Verschlüsselung zur Verfügung zu stellen, die kombinierte Funktionen zur Authentifizierung, Sicherung der Integrität, Zugriffssteuerung und Wahrung der Vertraulichkeit flexibel unterstützen. Aufgrund seiner leistungsfähigen Funktionen bei der Authentifizierung wurde dieser Standard von vielen Lieferanten von VPN-Produkten als Protokoll zum Aufbau sicherer Punkt-zu-Punkt-Verbindungen im Internet übernommen.

ISO. International Standards Organization.

ITU. International Telecommunication Union.

J

Java. Von Sun Microsystems, Incorporated, entwickelte plattformunabhängige Computertechnologien, die für den Netzbetrieb optimiert sind. Die Java-Umgebung besteht aus dem Java-Betriebssystem (Java-OS), den virtuellen Maschinen für verschiedene Plattformen, der

objektorientierten Java-Programmiersprache und einer Reihe von Klassenbibliotheken.

Java Virtual Machine (JVM). Der Teil der Java-Laufzeitumgebung, der zum Interpretieren von Bytecodes eingesetzt wird.

Java-Anwendung. Ein eigenständiges Programm, das in der Programmiersprache Java geschrieben ist. Es wird außerhalb eines Web-Browsers ausgeführt.

Java-Applet. *Siehe* Applet. *Gegensatz zu* Java-Anwendung.

Java-Klasse. Eine Einheit mit Java-Programmcode.

Java-Sprache. Eine von Sun Microsystems entwickelte Programmiersprache, die speziell für die Verwendung in Applet- und Agent-Anwendungen konzipiert wurde.

K

KeyStore (Schlüsselspeicher). Eine DL zum Speichern von Identitätsnachweisen für Trust Authority-Komponenten, z. B. Schlüssel und Zertifikate, in einem verschlüsselten Format.

Klartext. Nicht verschlüsselte Daten. *Synonym zu* unverschlüsselter Text.

Klasse. Beim objektorientierten Entwurf bzw. bei der objektorientierten Programmierung eine Gruppe von Objekten, die über eine gemeinsame Definition verfügen und aus diesem Grund mit denselben Merkmalen, Verarbeitungsoperationen und Funktionsweisen arbeiten.

Kryptographie. Bei der Sicherung von Computern die Prinzipien, Verfahren und Methoden zur Verschlüsselung von unverschlüsseltem und zur Entschlüsselung von verschlüsseltem Text.

L

LDAP. Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP). Ein Protokoll, mit dem auf das Directory zugegriffen werden kann.

Liste der ausgestellten Zertifikate (ICL). Eine vollständige Liste der ausgestellten Zertifikate sowie deren aktueller Status. Die Zertifikate sind anhand der Seriennummer und des Status indexiert. Diese Liste wird vom CA verwaltet und in der CA-Datenbank gespeichert.

M

MAC. Message Authentication Code - Nachrichtenauthentifizierungscode.

MD2. Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Sie wird zusammen mit MD5 in den PEM-Protokollen verwendet.

MD4. Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Ihre Geschwindigkeit übersteigt die von MD2 um ein Mehrfaches.

MD5. Eine unidirektionale Nachrichtenauszugs-Hash-Funktion, die von Ron Rivest entwickelt wurde. Sie stellt eine verbesserte Version von MD4 dar. MD5 verarbeitet Eingabetext in 512-Bit-Blöcken, die in 16 32-Bit-Unterblöcke aufgeteilt werden. Die Ausgabe des Algorithmus ist eine Gruppe von vier 32-Bit-Blöcken, die verkettet werden und so einen 128-Bit-Hash-Wert bilden. Diese Funktion wird ebenfalls zusammen mit MD2 in dem PEM-Protokollen verwendet.

Modulus. In dem auf öffentlichen Schlüsseln basierenden RSA-Verschlüsselungssystem das Produkt (`n`) aus zwei hohen Primzahlen: `p` und `q`. Die optimale Größe für einen RSA-Modulus hängt von den individuellen Sicherheitsanforderungen ab. Je größer der Modulus, desto höher die Sicherheit. Die momentan von den RSA Laboratories empfohlenen Schlüsselgrößen hängen vom geplanten Einsatz des Schlüssels ab. Hierbei werden 768 Bit für Schlüssel zum persönlichen Gebrauch, 1024 Bit für den Unternehmensbereich und 2048 Bit für extrem wertvolle Schlüssel wie z. B. CA-Schlüsselpaare angegeben. Ein 768-Bit-Schlüssel wird voraussichtlich bis mindestens zum Jahr 2004 sicher sein.

Multipurpose Internet Mail Extensions (MIME). Eine frei verfügbare Gruppe von Spezifikationen, die den Austausch von Text in Sprachen mit unterschiedlichen Zeichensätzen ermöglicht. Diese Spezifikationen unterstützen auch den Austausch von Multimedia-E-Mail zwischen unterschiedlichen Computersystemen, die Internet-Mail-Standards verwenden. So können E-Mail-Nachrichten beispielsweise andere Zeichensätze als den US-ASCII-Satz sowie erweiterten Text, Bilder oder Tondaten enthalten.

N

Nachrichtenauszug. Eine irreversible Funktion, bei der auf der Basis einer Nachricht beliebiger Länge eine Datenmenge mit fester Länge generiert wird. Bei MD5 handelt es sich z. B. um einen Nachrichtenauszugsalgorithmus.

Nachrichtenauthentifizierungscode (MAC). Ein geheimer Schlüssel, der von Sender und Empfänger gemeinsam benutzt wird. Der Sender authentifiziert sich und der Empfänger prüft die hierbei zur Verfügung gestellten Daten. Bei Trust Authority werden MAC-Schlüssel für CA- und Prüfkomponenten in den KeyStores gespeichert.

National Security Agency (NSA). Die offizielle Sicherheitsbehörde der US-Regierung.

NIST. National Institute of Standards and Technology, früher NBS (National Bureau of Standards). Aufgabe dieses Instituts ist die Unterstützung offener Standards und der Interoperabilität in den verschiedenen Bereichen der Computerbranche.

NLS. National Language Support - Unterstützung in der Landessprache.

NSA. National Security Agency.

O

Objekt. Beim objektorientierten Design oder bei der objektorientierten Programmierung eine abstrakte Entität, die zur Abgrenzung bestimmter Daten und der zugehörigen Operationen dient. *Siehe auch* Klasse.

Objekt-ID (OID). Ein von einer Verwaltungsfunktion zugeordneter Datenwert, der den in ASN.1 definierten Typ aufweist.

Objektart. Die Art von Objekt, die im Directory gespeichert werden kann. Beispiele sind eine Firma, ein Konferenzraum, eine Einheit, eine Person, ein Programm oder ein Prozeß.

ODBC. Open Database Connectivity.

Öffentlicher Schlüssel. In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel anderen Benutzern zur Verfügung. Er ermöglicht diesen Benutzern die Weiterleitung einer Transaktion an den Eigner des Schlüssels sowie die Prüfung einer digitalen Unterschrift. Mit einem öffentlichen Schlüssel verschlüsselte Daten können nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden. *Gegensatz zu* Privater Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Open Database Connectivity (ODBC). Ein Standard für den Zugriff auf unterschiedliche Datenbanksysteme.

Open Systems Interconnect (OSI). Der Name der von ISO genehmigten Computernetzstandards.

OSI. Open Systems Interconnect.

P

PC-Karte. Eine mit einer Smart-Card vergleichbare Einheit, die auch als PCMCIA-Karte bezeichnet wird. Sie ist etwas größer als eine Smart-Card und verfügt im allgemeinen über eine höhere Kapazität.

PEM. Privacy-Enhanced Mail.

PKCS. Public Key Cryptography Standards.

PKCS #1. *Siehe* Public Key Cryptography Standards.

PKCS #10. *Siehe* Public Key Cryptography Standards.

PKCS #11. *Siehe* Public Key Cryptography Standards.

PKCS #12. *Siehe* Public Key Cryptography Standards.

PKCS #7. *Siehe* Public Key Cryptography Standards.

PKI. Public Key Infrastructure.

PKIX. PKI auf X.509v3-Basis.

PKIX Certificate Management Protocol (PKIX CMP). Ein Protokoll, das Verbindungen mit PKIX-kompatiblen Anwendungen ermöglicht. PKIX CMP verwendet als primäres Transportverfahren TCP/IP, es ist jedoch eine Abstraktionsebene oberhalb der Sockets-Schicht vorhanden. Hierdurch können zusätzliche Datenübertragungsoperationen mit Sendeaufrufen (Polling) unterstützt werden.

PKIX CMP. PKIX Certificate Management Protocol.

PKIX-Empfangseinheit. Der öffentliche HTTP-Server, der von einer bestimmten Registrierungsdomäne verwendet wird, um Anforderungen der Client-Anwendung von Trust Authority zu empfangen.

Privacy-Enhanced Mail (PEM). Der vom Internet Architect Board (IAB) genehmigte Internet-Standard für die verbesserte Wahrung der Vertraulichkeit, der die sichere Übertragung elektronischer Post (E-Mail) über das Internet ermöglicht. Die PEM-Protokolle regeln Verschlüsselung, Authentifizierung, Nachrichtenintegrität und Schlüsselverwaltung.

Privater Schlüssel. In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel nur für seinen Eigner zur Verfügung. Er ermöglicht dem Eigner das Empfangen einer privaten Transaktion oder eine digitale Unterschrift. Die mit einem privaten Schlüssel unterzeichneten Daten können nur mit dem entsprechenden öffentlichen Schlüssel geprüft werden. *Gegensatz zu* Öffentlicher Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Protokoll. Eine vereinbarte Konvention für die Kommunikation zwischen Computern.

Protokollierungssubsystem. Bei Trust Authority ein Subsystem, das die Unterstützungsfunktionen zum Protokollieren von sicherheitsrelevanten Aktionen bereitstellt. Es entspricht den Empfehlungen, die im X9.57-Standard unter *Public Key Cryptography for the Financial Services Industry* definiert wurden.

Proxy-Server. Eine Einheit, die zwischen einem Computer, der eine Zugriffsanforderung absetzt (Computer A) und einem Computer, auf den zugegriffen werden soll (Computer B), implementiert ist. Wenn ein Endbenutzer eine Anforderung für eine Ressource über Computer A absetzt, wird diese an den Proxy-Server gelei-

tet. Dieser sendet die Anforderung an Computer B, erhält von diesem die Antwort und leitet diese an den Endbenutzer weiter. Mit Hilfe eines Proxy-Servers kann über einen Computer, der sich innerhalb einer Firewall befindet, auf das World Wide Web zugegriffen werden.

Prüf-Client. Jeder Client im System, der Prüfereignisse an den Trust Authority-Prüf-Server sendet. Bevor ein Prüf-Client ein Ereignis an den Prüf-Server sendet, stellt er eine Verbindung zu diesem her. Nach der Herstellung der Verbindung verwendet der Client die Client-Bibliothek des Prüfsubsystems, um Ereignisse an den Prüf-Server zu übertragen.

Prüf-Server. Ein Trust Authority-Server, der zum Empfangen von Prüfereignissen von Prüf-Clients und zum Aufzeichnen dieser Ereignis in einem Prüfprotokoll dient.

Prüfprotokoll. Daten in Form eines logischen Pfades, die eine Folge von Ereignissen verbinden. Mit dem Prüfprotokoll können Transaktionen oder der bisherige Verlauf einer bestimmten Aktivität verfolgt werden.

Prüfprotokoll. Bei Trust Authority eine Tabelle in einer Datenbank, in der für jedes Prüfereignis ein Datensatz gespeichert wird.

Prüfzeichenfolge. Eine Zeichenfolge, die von einem Server oder einer Anwendung gesendet wird und zum Anfordern der Benutzerberechtigung dient. Der Benutzer, der zur Authentifizierung aufgefordert wird, unterzeichnet die Prüfzeichenfolge mit einem privaten Schlüssel. Der öffentliche Schlüssel des Benutzers sowie die unterzeichnete Prüfzeichenfolge werden zurück an den Server oder die Anwendung gesendet, der bzw. die die Authentifizierung anforderte. Der Server versucht anschließend, die unterzeichnete Prüfzeichenfolge mit Hilfe des öffentlichen Schlüssels des Benutzers zu entschlüsseln. Wenn die entschlüsselte Prüfzeichenfolge mit der ursprünglich gesendeten Prüfzeichenfolge übereinstimmt, gilt der Benutzer als authentifiziert.

Public Key Cryptography Standards (PKCS). Informelle, herstellerübergreifende Standards, die im Jahr 1991 von den RSA Laboratories in Zusammenarbeit mit Repräsentanten verschiedener Computerhersteller entwickelt wurden. Diese Standards umfassen die RSA-Verschlüsselung, die Diffie-Hellman-Vereinbarung, die kennwortbasierte Verschlüsselung sowie die Syntax für erweiterte Zertifikate, verschlüsselte Nachrichten, Daten zu privaten Schlüsseln und für die Zertifizierung.

- PKCS #1 beschreibt ein Verfahren zum Verschlüsseln von Daten mit Hilfe des RSA-Verschlüsselungssystems auf der Basis öffentlicher Schlüssel. Er dient zur Erstellung digitaler Unterschriften und Briefumschläge.
- PKCS #7 definiert ein allgemeines Format für verschlüsselte Nachrichten.
- PKCS #10 definiert eine Standardsyntax für Zertifizierungsanforderungen.
- PKCS #11 definiert eine Programmierschnittstelle für Verschlüsselungseinheiten, z. B. Smart-Cards, die unabhängig vom verwendeten technologischen Konzept ist.
- PKCS #12 definiert ein portierbares Format zum Speichern oder Transportieren der privaten Schlüssel, Zertifikate und sonstiger geheimer Daten etc. eines Benutzers.

Public Key Infrastructure (PKI). Ein Standard für Sicherheitssoftware, der auf der Verschlüsselung mit Hilfe öffentlicher Schlüssel basiert. Bei PKI handelt es sich um ein System digitaler Zertifikate, Zertifikatsaussteller, Registrierungsstellen, Zertifikatverwaltungsservices und verteilter Verzeichnisservices. Er dient zum Prüfen der Identität und Berechtigung aller Parteien, die an Transaktionen beteiligt sind, die über das Internet ausgeführt werden. Diese Transaktionen umfassen möglicherweise Operationen, zu deren Ausführung eine Identitätsprüfung erforderlich ist. Sie dienen z. B. zur Bestätigung des Ursprungs von Senderechtanforderungen, E-Mail-Nachrichten oder Finanztransaktionen.

PKI erreicht dieses Ziel dadurch, daß öffentliche Chiffrierschlüssel und Benutzerzertifikate für die Authentifizierung durch eine berechtigte Einzelperson oder ein berechtigtes Unternehmen verfügbar gemacht werden. Er stellt Online-Verzeichnisse bereit, die die öffentlichen Chiffrierschlüssel und Zertifikate enthalten, die zur Überprüfung der digitalen Zertifikate, Identitätsnachweise sowie der digitalen Unterschriften verwendet werden.

PKI stellt außerdem Funktionen zur schnellen und effizienten Antwort auf Prüfabfragen und Anforderungen für öffentliche Chiffrierschlüssel bereit. Der Standard dient darüber hinaus zur Identifizierung potentieller Sicherheitslücken im System und zur Verwaltung von Ressourcen zur Bearbeitung von Sicherheitsverletzungen. PKI bietet außerdem einen digitalen Zeitmarkenservice für wichtige Unternehmenstransaktionen.

R

RA. Registration Authority - Registrierungsstelle.

RA Desktop. Ein Java-Applet, das den RAs eine Grafikschnittstelle für die Verarbeitung von Anforderungen für Identitätsnachweise und zur Verwaltung dieser Nachweise während ihrer Gültigkeitsdauer zur Verfügung stellt.

RA-Server. Der Server für die RA-Komponente von Trust Authority.

RC2. Eine variable Schlüsselgrößen-Block-Cipher, die von Ron Rivest für RSA Data Security entwickelt wurde. *RC* steht für *Ron's Code* oder *Rivest's Cipher*. Sie arbeitet schneller als DES und löst diese Block-Cipher ab. Durch die Verwendung geeigneter Schlüsselgrößen

kann sie in Bezug auf eine ausgedehnte Schlüsselsuche flexibler als DES gestaltet werden. Sie verfügt über eine Blockgröße von 64 Bit und arbeitet auf Softwareebene zwei- bis dreimal schneller als DES. RC2 kann in denselben Modi eingesetzt werden wie DES.

Durch eine Vereinbarung zwischen SPA (Software Publishers Association) und der US-Regierung nimmt RC2 einen speziellen Status ein. Hierdurch ist das Genehmigungsverfahren für den Export einfacher und schneller, als dies bei anderen Verschlüsselungsprodukten der Fall ist. Um die Voraussetzungen für eine rasche Exportgenehmigung zu erfüllen, muß ein Produkt mit einigen Ausnahmen die RC2-Schlüsselgröße auf 40 Bit beschränken. Eine zusätzliche Zeichenfolge kann verwendet werden, um Nichtberechtigte abzuwehren, die versuchen, eine umfangreiche Tabelle möglicher Verschlüsselungsvarianten vorauszuberechnen.

Regel-Exit. In einer Registrierungsfunktion ein auf Unternehmensebene definiertes Programm, das von der Registrierungsanwendung aufgerufen wird. Die Regeln eines Regel-Exits implementieren die Unternehmens- und Sicherheitsbenutzervorgaben eines Unternehmens für den Registrierungsprozeß.

Registrator. Ein Benutzer, der für den Zugriff auf RA Desktop sowie zur Verwaltung und Anforderung von Zertifikaten berechtigt ist.

Registrierter Name (DN). Der eindeutige Name eines im Directory gespeicherten Dateneintrags. Der DN dient zur eindeutigen Identifizierung der Position eines Eintrags in der hierarchischen Struktur des Directory.

Registrierung. Bei Trust Authority das Abrufen von Identitätsnachweisen für die Verwendung über das Internet. Bei der Registrierung werden Zertifikate angefordert, erneuert und widerrufen.

Registrierungsattribut. Eine Registrierungsvariable, die in einem Registrierungsformular enthalten ist. Ihr Wert gibt die Informationen wider, die während der Registrierung erfaßt werden. Der Wert des Registrierungsattributs bleibt während der gesamten Gültigkeitsdauer des Identitätsnachweises gleich.

Registrierungsdatenbank. Diese Datenbank enthält Informationen zu Zertifikatsanforderungen und ausgestellten Zertifikaten. In der Datenbank werden Registrierungsdaten gespeichert und alle Änderungen aufgezeichnet, die während der Gültigkeitsdauer an einem Zertifikat vorgenommen werden. Die Datenbank kann durch RA-Prozesse und Regel-Exits oder durch den Registrator aktualisiert werden.

Registrierungsdomäne. Eine Gruppe von Ressourcen, Regeln und Konfigurationsoptionen, die sich auf bestimmte Registrierungsprozesse für Zertifikate beziehen. Der Domänenname stellt einen untergeordneten Wert zur URL-Adresse dar, die zur Ausführung der Registrierungsfunktion eingesetzt wird.

Registrierungsfunktion. Ein Trust Authority-Anwendungsgerüst, das spezielle Verfahren zur Registrierung von Entitäten (z. B. Browser, Router, E-Mail-Einheiten und sichere Client-Anwendungen) und zur Verwaltung von Zertifikaten während ihrer Gültigkeitsdauer bereitstellt.

Registrierungsprozeß. Bei Trust Authority die Schritte, die zur Überprüfung eines Benutzers ausgeführt werden. Durch den Registrierungsprozeß werden Benutzer sowie deren öffentliche Schlüssel zertifiziert, um sie zur Teilnahme an den gewünschten Transaktionen zu berechtigen. Er kann lokal oder Web-gestützt, automatisch oder von einer tatsächlich mit Personen besetzten Registrierungsstelle ausgeführt werden.

Registrierungsstelle (RA). Die Software, die zur Verwaltung digitaler Zertifikate verwendet wird und sicherstellt, daß die Unternehmensregeln vom ersten Empfang einer Registrierungsanforderung bis zum Zertifikatswiderruf angewendet werden.

Registrierungsvariable. *Siehe* Registrierungsattribut.

RSA. Ein auf öffentlichen Schlüsseln basierender Verschlüsselungsalgorithmus, der nach seinen Erfindern (Rivest, Shamir und Adelman) benannt wurde. Er wird zur Verschlüsselung und für digitale Unterschriften verwendet.

S

S/MIME. Ein Standard, der das Unterzeichnen und Verschlüsseln von elektronischer Post (E-Mail) unterstützt, die über das Internet übertragen wird. *Siehe* MIME.

Schema. Beim Directory die interne Struktur, die zur Definition der Beziehungen zwischen den verschiedenen Objektarten verwendet wird.

Schlüssel. Bei der Verschlüsselung ein Wert, der zum Ver- und Entschlüsseln von Informationen verwendet wird.

Schlüsselpaar. Zusammengehörende Schlüssel, die bei der asymmetrischen Verschlüsselung eingesetzt werden. Ein Schlüssel wird zur Verschlüsselung, der andere zur Entschlüsselung verwendet.

Schlüsselpaar aus öffentlichem und privatem Schlüssel. Ein Schlüsselpaar aus öffentlichem und privatem Schlüssel stellt ein grundlegendes Element der Verschlüsselung auf der Basis von Schlüsselpaaren dar. (Diese Form der Verschlüsselung wurde im Jahr 1976 von Whitfield Diffie und Martin Hellman eingeführt, um Probleme bei der Schlüsselverwaltung zu lösen.) Nach diesem Konzept erhält jeder Benutzer ein Schlüsselpaar, bei dem einer als öffentlicher und einer als privater Schlüssel bezeichnet wird. Der öffentliche Schlüssel ist hierbei allgemein bekannt, der private Schlüssel wird hingegen geheimgehalten. Sender und

Empfänger müssen geheime Daten nicht gemeinsam benutzen. Alle Kommunikationsoperationen werden lediglich auf der Basis öffentlicher Schlüssel ausgeführt. Die privaten Schlüssel werden niemals übertragen oder gemeinsam verwendet. Auf diese Weise ist es nicht mehr notwendig, sich auf die Sicherheit eines Übertragungskanals gegenüber Manipulationen zu verlassen. Die einzige Anforderung ist, daß öffentliche Schlüssel den entsprechenden Benutzern in einer gesicherten (authentifizierten) Weise (z. B. in einem gesicherten Verzeichnis) zugeordnet werden. Jeder Benutzer kann nun mit Hilfe dieser öffentlichen Daten eine vertrauliche Nachricht senden. Diese Nachricht kann nur mit einem privaten Schlüssel entschlüsselt werden, auf den allein der gewünschte Empfänger zugreifen kann. Darüber hinaus kann die Verschlüsselung auf der Basis von Schlüsselpaaren nicht nur zur Gewährleistung der Vertraulichkeit (Verschlüsselung), sondern auch für die Authentifizierung (digitale Unterschriften) eingesetzt werden.

Secure Electronic Transaction (SET). Ein Branchenstandard für die Durchführung sicherer Kredit- oder Kundenkartenzahlungen über nicht gesicherte Netze. Der Standard formuliert Definitionen für die Authentifizierung von Kartenhaltern, Händlern sowie der Banken, durch die die Karten ausgestellt werden, da er die Ausstellung von Zertifikaten anfordert.

Secure Sockets Layer (SSL). Ein IETF-Standardübertragungsprotokoll mit integrierten Sicherheitsservices, die für den Endbenutzer möglichst transparent sind. Es stellt einen digitalen, sicheren Kommunikationskanal zur Verfügung.

Ein SSL-fähiger Server empfängt SSL-Verbindungsanforderungen im allgemeinen an einem anderen Anschluß (Port) als normale HTTP-Anforderungen. SSL erstellt eine Sitzung, in der die Austauschsignale zum Herstellen der Kommunikation zwischen zwei Modems nur einmal gesendet werden müssen. Anschließend wird die Kommunikation verschlüsselt und die Nachrichtenintegrität wird solange überprüft, bis die SSL-Sitzung abgelaufen ist.

Server. (1) In einem Netz eine Datenstation, die anderen Stationen Funktionen zur Verfügung stellt, wie beispielsweise ein Datei-Server. (2) In TCP/IP ein System in einem Netz, das die Anforderungen eines Systems an einem anderen Standort verarbeitet. Dieses Konzept wird als Client/Server-Modell bezeichnet.

Server-Zertifikat. Ein digitales Zertifikat, das von einem CA ausgegeben wird und es einem Web-Server ermöglicht, SSL-gestützte Transaktionen auszuführen. Wenn ein Browser über das SSL-Protokoll eine Verbindung zum Server herstellt, sendet der Server seinen öffentlichen Schlüssel an den Browser. Hierdurch kann die Identität des Servers authentifiziert werden und es können verschlüsselte Daten an den Server gesendet werden. *Siehe auch* CA-Zertifikat, Digitales Zertifikat, *und* Browser-Zertifikat.

Servlet. Ein Server-Programm, das zusätzliche Funktionen für Server zur Verfügung stellt, die Java unterstützen.

SET. Secure Electronic Transaction.

SGML. Standard Generalized Markup Language.

SHA-1 (Secure Hash Algorithm). Ein von NIST und NSA entwickelter Algorithmus, der beim DSS (Digital Signature Standard) verwendet wird. Der Standard wird als Secure Hash Standard bezeichnet; SHA ist der Algorithmus, der von diesem Standard verwendet wird. Er generiert einen 160-Bit-Hash-Code.

Sicherheitsdomäne. Eine Gruppe (z. B. Unternehmen, Arbeitsgruppe, Projektteam), deren Zertifikate vom gleichen CA zertifiziert wurden. Benutzer, die über ein von einem CA unterzeichnetes Zertifikat verfügen, können der Identität eines anderen Benutzers vertrauen, der ein Zertifikat besitzt, das vom selben CA unterzeichnet worden ist.

Sicherungsmodell. Eine Organisationskonvention, die regelt, wie Zertifikatsaussteller (CAs) andere Zertifikatsaussteller zertifizieren können.

Simple Mail Transfer Protocol (SMTP). Ein Protokoll, mit dem elektronische Post über das Internet übertragen wird.

Site-Zertifikat. Dieser Zertifikatstyp ist mit einem CA-Zertifikat vergleichbar, gilt jedoch nur für eine bestimmte Website. *Siehe auch* CA-Zertifikat.

Smart-Card. Eine Hardwarekomponente, normalerweise in der Größe einer Kreditkarte, auf der die digitalen Schlüssel eines Benutzers gespeichert werden können. Eine Smart-Card kann kennwortgeschützt werden.

SMTP. Simple Mail Transfer Protocol.

SSL. Secure Sockets Layer.

Standard Generalized Markup Language (SGML). Ein Standard zur Beschreibung von Formatierungssprachen. HTML basiert auf SGML.

Symmetrische Verschlüsselung. Eine Form der Verschlüsselung, bei der sowohl für die Ver- als auch für die Entschlüsselung derselbe Schlüssel verwendet wird. Die Sicherheit dieses Verfahren basiert auf dem Schlüssel. Wird dieser öffentlich bekanntgegeben, können die mit ihm bearbeiteten Nachrichten von jedem Benutzer ver- und entschlüsselt werden. Der Inhalt der übertragenen Daten kann nur dann geheimgehalten werden, wenn der Schlüssel nur den jeweils berechtigten Personen bekannt ist. *Gegensatz zu* Asymmetrische Verschlüsselung.

Symmetrischer Schlüssel. Ein Schlüssel, der sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet werden kann. *Siehe auch* Symmetrische Verschlüsselung.

T

TCP/IP. Transmission Control Protocol/Internet Protocol.

TP. Trust Policy = Sicherungsregel.

Transaktions-ID. Eine Kennung, die die RA als Antwort auf eine Anforderung für eine Vorabregistrierung zur Verfügung stellt. Mit dieser ID kann ein Benutzer, der die Client-Anwendung von Trust Authority ausführt, ein vorab genehmigtes Zertifikat erhalten.

Transmission Control Protocol/Internet Protocol (TCP/IP). Eine Gruppe von Übertragungsprotokollen, die Peer-zu-Peer-Konnektivitätsfunktionen für lokale Netze (LANs) und Weitverkehrsnetze (WANs) unterstützen.

Triple DES. Ein symmetrischer Algorithmus, bei dem der unverschlüsselte Text dreimal verschlüsselt wird. Obwohl für diese Mehrfachverschlüsselung zahlreiche Methoden existieren, stellt die Triple DES-Verschlüsselung, die auf drei verschiedenen Schlüsseln basiert, das sicherste dieser Verfahren dar.

Trust Authority. Eine integrierte IBM SecureWay-Sicherheitslösung, die die Ausstellung, Erneuerung und den Widerruf digitaler Zertifikate unterstützt. Diese Zertifikate können für eine breite Palette von Internet-Anwendungen eingesetzt werden und bieten eine Möglichkeit zur Authentifizierung von Benutzern und zur Gewährleistung einer gesicherten Kommunikation.

Tunnel. In der VPN-Technologie eine virtuelle Punkt-zu-Punkt-Verbindung, die auf Anfrage über das Internet hergestellt wird. Während der Verbindung können ferne Benutzer den Tunnel verwenden, um sichere, verschlüsselte und gekapselte Informationen mit Servern im privaten Netz eines Unternehmens auszutauschen.

U

Unbestreitbarkeit. Die Verwendung eines digitalen, privaten Schlüssels, um zu verhindern, daß der Unterzeichner eines Dokuments dessen Unterzeichnung leugnet.

Unicode. Ein 16-Bit-Zeichensatz, der in ISO 10646 definiert ist. Der Unicodestandard für die Verschlüsselung von Zeichen ist ein internationaler Zeichencode für die Informationsverarbeitung. Er umfaßt die grundlegenden, weltweit verwendeten Prozeduren und bildet die Basis für die Internationalisierung und Lokalisierung von Software. Der gesamte Quellencode in der Java-Programmierungsumgebung wird in Unicode geschrieben.

Unternehmensprozeßobjekte. Eine Codegruppe, die zur Ausführung einer bestimmten Registrierungsoperation, z. B. zum Prüfen des Registrierungsstatus oder zur Bestätigung des Sendens eines öffentlichen Schlüssels, verwendet wird.

Unternehmensprozeßschablone. Eine Gruppe von Unternehmensprozeßobjekten, die in einer bestimmten Reihenfolge ausgeführt werden.

Unterstützung in der Landessprache (NLS). Unterstützung für unterschiedliche länderspezifische Angaben in einem Produkt. Hierzu gehören die Sprache, die Währung, das Datums- und Zeitformat und die Darstellung von Zahlen.

Unterzeichnen. Die Verwendung eines digitalen privaten Schlüssels zum Generieren einer Unterschrift. Diese Unterschrift dient dazu, zu beweisen, daß ein bestimmter Benutzer für die von ihm unterzeichnete Nachricht verantwortlich ist und diese akzeptiert.

Unterzeichnen/Prüfen. Als Unterzeichnen wird die Verwendung eines privaten Schlüssels zum Generieren einer Unterschrift bezeichnet. Unter Prüfen versteht man die Verwendung des entsprechenden öffentlichen Schlüssels zur Verifizierung dieser Unterschrift.

Unverschlüsselter Text. Nicht verschlüsselte Daten. *Synonym zu* Klartext.

URL. Uniform Resource Locator - URL-Adresse.

URL-Adresse. Ein Schema für die Adressierung von Ressourcen im Internet. Die URL-Adresse gibt das verwendete Protokoll sowie den Host-Namen und die IP-Adresse an. Außerdem enthält er Angaben zur Anschlußnummer, zum Pfad sowie weitere Ressourcendetails, die erforderlich sind, um über eine bestimmte Maschine auf eine Ressource zuzugreifen.

UTF-8. Ein Umsetzungsformat. Es ermöglicht Informationsverarbeitungssystemen, die nur die Verarbeitung von 8-Bit-Zeichensätzen unterstützen, die Umsetzung von 16-Bit-Unicode in ein 8-Bit-Äquivalent und umgekehrt, ohne daß hierbei Informationen verlorengehen.

V

Verkettungsprüfung. Die Gültigkeitsprüfung aller CA-Unterschriften in der Trust-Hierarchie, über die ein bestimmtes Zertifikat ausgestellt wurde. Wenn z. B. das Unterschriftszertifikat eines CA über einen anderen CA ausgestellt wurde, werden bei der Gültigkeitsprüfung des vom Benutzer vorgelegten Zertifikats beide Unterschriften geprüft.

Verschlüsseln. Das Umordnen von Informationen, so daß nur Personen, die über den richtigen Entschlüsselungscode verfügen, die ursprünglichen Informationen durch Entschlüsselung abrufen können.

Verschlüsselt. Die Eigenschaft von Daten, die nach einem bestimmten System umgesetzt wurden, um deren Bedeutung unkenntlich zu machen.

Verschlüsselung/Entschlüsselung. Die Verwendung des öffentlichen Schlüssels des gewünschten Empfängers zum Verschlüsseln von Daten für diese Person. Der Empfänger verwendet anschließend den privaten Schlüssel seines Schlüsselpaares, um die Daten zu entschlüsseln.

Vertrauensdomäne. Eine Gruppe von Entitäten, deren Zertifikate vom gleichen CA zertifiziert wurden.

Vertraulichkeit. Die Wahrung der Geheimhaltung bestimmter Informationen gegenüber nicht berechtigten Personen.

Vertraulichkeit. Der Schutz von Daten gegen den Zugriff nicht berechtigter Personen.

Virtual Private Network (VPN). Ein privates Datennetz, das ferne Verbindungen nicht über Telefonleitungen, sondern über das Internet herstellt. Da der Zugriff der Benutzer auf die Netzressourcen eines Unternehmens nicht über eine Telefongesellschaft, sondern über einen Internet Service Provider (ISP) erfolgt, können diese durch den Einsatz von VPN deutliche Einsparungen bei Fernzugriffen erzielen. Ein VPN erhöht auch die Sicherheit beim Datenaustausch. Bei der herkömmlichen Firewall-Technologie kann zwar der Inhalt der Nachricht verschlüsselt werden, nicht jedoch die Quellen- und Zieladressen. Bei der VPN-Technologie können die Benutzer eine Tunnelverbindung herstellen, bei der das gesamte Datenpaket (Header- und Datenkomponente) verschlüsselt und gekapselt ist.

Vorabregistrierung. Bei Trust Authority ein Prozeß, mit dem ein bestimmter Benutzer (normalerweise ein Administrator) andere Benutzer registrieren kann. Wenn die Anforderung genehmigt wird, stellt die RA Informationen zur Verfügung, mit denen der Benutzer später mit Hilfe der Client-Anwendung von Trust Authority ein Zertifikat erhalten kann.

VPN. Virtual Private Network.

W

Web-Browser. Auf einem PC ausgeführte Client-Software, mit der ein Benutzer im World Wide Web navigieren oder lokale HTML-Seiten anzeigen kann. Der Web-Browser ist ein Abfrage-Tool, das universellen Zugriff auf die umfangreichen Hypermedia-Datensammlungen ermöglicht, die im Web und im Internet zur Verfügung gestellt werden. Manche Browser können Text und Grafik anzeigen, während andere Browser auf die Textanzeige beschränkt sind. Die meisten Browser unterstützen die Hauptformen der Internet-Kommunikation, z. B. die Ausführung von FTP-Transaktionen.

Web-Server. Ein Server-Programm, das auf Anforderungen von Browser-Programmen nach Informationsressourcen antwortet. *Siehe auch* Server.

WebSphere Application Server. Ein IBM Produkt, das Benutzer bei der Entwicklung und Verwaltung von Websites mit einem hohen Leistungsumfang unterstützt. Es erleichtert den Übergang vom einfachen Web Publishing zu komplexen e-business-Anwendungen im Web. Der WebSphere Application Server besteht aus einer Java-Servlet-Maschine, die unabhängig vom Web-Server und dem verwendeten Betriebssystem arbeitet.

World Wide Web (WWW). Der Teil des Internets, in dem ein Netz von Verbindungen zwischen Computern aufgebaut wird, auf denen Hypermediamaterial gespeichert ist. Dieses Material stellt neben Informationen auch Verbindungen (Hyperlinks) zu anderem Material im World Wide Web und Internet zur Verfügung. Der Zugriff auf WWW-Ressourcen erfolgt über einen Web-Browser.

X

X.500. Ein Standard für die Implementierung eines multifunktionalen, verteilten und vervielfältigten Verzeichnisservices durch die Verbindung von Computersystemen. Dieser Standard wurde gemeinsam definiert von der bisher als CCITT bekannten International Telecommunications Union (ITU) sowie der International Organization for Standardization und der International Electro-Chemical Commission (ISO/IEC).

X.509 Version 3-Zertifikat. Das X.509v3-Zertifikat verfügt über erweiterte Datenstrukturen für die Speicherung und das Abrufen von Informationen zu Zertifikatsanträgen, zur Zertifikatsverteilung und zu Zertifikatswiderrufen sowie zu Sicherheitsregeln und digitalen Unterschriften.

X.509v3-Prozesse dienen zum Erstellen von CRLs mit Zeitmarken für alle Zertifikate. Bei jeder Verwendung eines Zertifikats ermöglichen die X.509v3-Funktionen der Anwendung, die Gültigkeit des Zertifikats zu überprüfen. Die Anwendung kann außerdem feststellen, ob sich das Zertifikat auf der Zertifikatswiderrufsliste (CRL) befindet. CRLs unter X.509v3 können für eine bestimmte Gültigkeitsperiode erstellt werden. Sie können auch auf anderen Kriterien basieren, die zur Aufhebung der Gültigkeit eines Zertifikats führen. Wenn z. B. ein Mitarbeiter ein Unternehmen verläßt, wird sein Zertifikat in der CRL eingetragen.

X.509-Zertifikat. Ein weitverbreiteter Zertifikatsstandard, der entwickelt wurde, um die sichere Verwaltung und Verteilung von digital unterzeichneten Zertifikaten

über sichere Internet-Netze zu unterstützen. Das X.509-Zertifikat definiert Datenstrukturen, die Prozeduren für die Verteilung öffentlicher Schlüssel unterstützen, die von zuverlässigen Stellen digital unterzeichnet sind.

Z

Zertifikatsaussteller (CA). Die Software, die zur Einhaltung der Sicherheitsregeln eines Unternehmens und zur Vergabe gesicherter elektronischer Identitäten in Form von Zertifikaten dient. Der CA verarbeitet die Anforderungen von RAs zum Ausstellen, Erneuern und Widerrufen von Zertifikaten. Er kooperiert mit der RA, um Zertifikate und CRLs im Directory zu veröffentlichen. *Siehe auch* Digitales Zertifikat.

Zertifikatserweiterung. Eine Zusatzfunktion des X.509v3-Zertifikatformats, die zur Einbindung zusätzlicher Felder in das Zertifikat dient. Es stehen Standard- und benutzerdefinierte Erweiterungen zur Verfügung. Die Standarderweiterungen dienen verschiedenen Zwecken und umfassen Schlüssel- und Regelinformationen, Betreff- und Ausstellerattribute sowie Einschränkungen, die für den Zertifizierungspfad gelten.

Zertifikatsprofil. Eine Gruppe von Kenndaten, die den gewünschten Zertifikatstyp definieren (z. B. SSL- oder IPSec-Zertifikate). Das Profil vereinfacht die Zertifikatsspezifikation und -registrierung. Der Aussteller kann die Namen der Profile ändern und Kenndaten des gewünschten Zertifikats angeben. Hierzu zählen z. B. der Gültigkeitszeitraum, die Verwendung von Schlüsseln, DN-Einschränkungen usw.

Zertifikatsregel. Eine benannte Gruppe mit Regeln, die angibt, ob ein Zertifikat für eine bestimmte Klasse von Anwendungen mit gemeinsamen Sicherheitsanforderungen anwendbar ist. Eine Zertifikatsregel kann z. B. angeben, ob ein bestimmter Zertifizierungstyp dem Benutzer die Ausführung von Transaktionen für Waren innerhalb eines bestimmten Preisbereichs ermöglicht.

Zertifikatswiderrufsliste (CRL). Eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. Die Zertifikate in dieser Liste sollten als nicht akzeptierbar behandelt werden. *Siehe auch* Digitales Zertifikat.

Zertifizierung. Der Prozeß, bei dem eine zuverlässige, an der Kommunikation nicht beteiligte Stelle (der Zertifikatsaussteller - CA) einen elektronischen Identitätsnachweis ausstellt, der für die Identität einer Person, eines Unternehmens oder einer Organisation bürgt.

Ziel. Eine benannte oder ausgewählte Datenquelle.

Zugriffssteuerungsliste (ACL). Ein Verfahren, mit dem die Verwendung einer bestimmten Ressource auf berechtigte Benutzer beschränkt werden kann.

Index

A

Abschnitte, Registrierungsformular 6, 7, 9
Algorithmen für Unterschriften 46
Anforderung, Registrierung 3
  auswerten 26
  automatisierte Auswertung 26
  Bearbeitung durch RA 3
  Registrierungsdatenbanksatz 28
  Registrierungsdomäne 27
  Registrierungsformular 25
  über Client-Anwendung 17
  über die Registrierungs-Web-Seite 5
  Verarbeitungszyklus 28
  Vorabregistrierung 25
  Web-Browser-Unterstützung 26
Anforderung in Client-Anwendung löschen 18
Anforderungs-ID 6, 7, 9
Anstehende Anforderung, Client-Anwendung 18
Attribute, Datenbanksatz 28
Authentifizierung 31

B

Begründung für den Widerruf 37
Beschädigter Schlüssel 37
Browser-Unterstützung 26
Browser-Voraussetzungen 38
Browser-Zertifikat 29
Browser-Zertifikatsanforderung 6

C

CA-Hierarchie 28
CA-Zertifikat 5, 29
Client-Anwendung 3
  deinstallieren 24
  eine physische Smart Card aktivieren 15
  installieren 14
  Registrierung 17
  Systemvoraussetzungen 38
  Szenario für den Zertifikatsabruf 25
  verlassen 24
  Zertifikate verwalten 18
  Zugriff 16
Client-Anwendung - Fensterelemente 39
Client-Anwendung - Registrierung 17
  mit Transaktions-ID 17
  mit Vorabregistrierungsdatei 17
Client-Anwendung, Dialog 40
  Datei unterzeichnen 46
  Kennwort ändern 41
  Neues Zertifikat unter Verwendung einer Transaktions-ID 43
  Neues Zertifikat unter Verwendung einer Vorabregistrierungsdatei 42
  Smart Card-Eigenschaften 46
  Smart Card öffnen 44
Client-Anwendung, Dialog 40 *(Forts.)*
  Zertifikat erneuern 45
  Zertifikat exportieren 42
  Zertifikat importieren 42
  Zertifikat löschen 41
  Zertifikat öffnen 43
  Zertifikat widerrufen 45
  Zertifikatserneuerung 41
Client-Anwendungsanforderung löschen 18

D

Dateien unterzeichnen 21
Datenbanksätze, Registrierung 3, 27, 28
  Attribute 28
  Bearbeitung durch RA 3
DB2 27
Deinstallierung der Client-Anwendung 24
Demnächst ablaufende Zertifikate 20, 41
Details zu Zertifikaten 19
Dialog 40
  Datei unterzeichnen 46
  Kennwort ändern 41
  Neues Zertifikat unter Verwendung einer Transaktions-ID 43
  Neues Zertifikat unter Verwendung einer Vorabregistrierungsdatei 42
  Smart Card-Eigenschaften 46
  Smart Card öffnen 44
  Zertifikat erneuern 45
  Zertifikat exportieren 42
  Zertifikat importieren 42
  Zertifikat löschen 41
  Zertifikat öffnen 43
  Zertifikat widerrufen 45
  Zertifikatserneuerung 41
Dialog 'Datei unterzeichnen' 46
Dialog 'Kennwort ändern' 41
Dialog 'Neues Zertifikat unter Verwendung einer Transaktions-ID' 43
Dialog 'Neues Zertifikat unter Verwendung einer Vorabregistrierungsdatei' 42
Dialog 'Smart Card-Eigenschaften' 46
Dialog 'Smart Card öffnen' 44
Dialog 'Zertifikat erneuern' 45
Dialog 'Zertifikat exportieren' 42
Dialog 'Zertifikat importieren' 42
Dialog 'Zertifikat löschen' 41
Dialog 'Zertifikat öffnen' 43
Dialog 'Zertifikat widerrufen' 45
Dialog 'Zertifikatserneuerung' 41
Digitale Unterschriften 21, 31
Digitales Zertifikat 29
  Anforderung über die Registrierungs-Web-Seite 5
  aus einer Datei importieren 19
  Datenbanksätze 27
  demnächst ablaufend 20, 41
  Details 19
Digitales Zertifikat 29 *(Forts.)*
  erneuerbar 30
  in eine Datei exportieren 18
  Kategorien 29
  löschen 18
  nicht erneuerbar 30
  Typen 36
  über Client-Anwendung anfordern 17
  über Client-Anwendung verwalten 18
  Verwaltung über die Registrierungs-Web-Seite 11
  zur Verwendung der Registrierungsservices 5, 29
  zusammenfassende Informationen 22
Directory-Zugriff 28

E

E-Mail-Benachrichtigung 6, 7, 9, 33
Eigenschaften, Smart Card 24
Einheitenzertifikat 7, 30
Erläuterungen, Abschnitte 25
Erneuerbares Zertifikat 30
Erneuerbarkeit 30
Erneuerung
  über Client-Anwendung 20
  über die Registrierungs-Web-Seite 12

G

Gegenseitige Zertifizierung 28
Geschäftsprozeßvariablen 30
Gesicherte Anwendungen 31
Gesicherte Ressourcen 3, 31
Gültigkeitszeitraum 36

H

Hilfe für die Client-Anwendung 47

I

Identifikationsprüfungsantwort 6, 7, 9, 10, 33
Informationen zur Vorgehensweise, Abschnitte 5
initsc, Programm 15
Installieren der Client-Anwendung 14
Internet Explorer - Browser-Zertifikat 6

L

LDAP-Protokoll 28
Liste der Zertifikate 22
Löschen einer Anforderung, Client-Anwendung 18

M

MD5 With RSA, Algorithmus 46
Menüs, Fenster 'Smart Card' 39

N

Netscape - Browser-Zertifikat 6
Nicht erneuerbares Zertifikat 30

P

Physische Smart Cards aktivieren 15
PKCS #10-Anforderung für Zertifikate 30, 33
PKIX-kompatible Anwendung 9, 29
Protokoll, Directory-Zugriff 28
Protokolle 29

R

RA 27
RA Desktop 25, 27
Referenzinformationen, Abschnitte 33
Registerkarten, Fenster 'Smart Card' 22, 40
Registrator 25, 26, 27
Registrierter Name 29
Registrierung 26
  automatisiert 26
  Bedarf 3
  Regeln 27
  Systemvoraussetzungen 38
  über die Client-Anwendung 17
  über die Registrierungs-Web-Seite 5
  Web-Browser-Unterstützung 26
Registrierung, Client-Anwendung
  mit Transaktions-ID 17
  mit Vorabregistrierungsdatei 17
Registrierungs-Web-Seite 3, 5
  Anforderungs-ID 6, 7, 9
  Anforderungsstatus überprüfen 10
  CA-Zertifikat 29
  Felder des Registrierungsformulars 33
  Registrierungsarten 25
  Szenario für die Vorabregistrierung 25
  URL 5
  Zugriff 5
Registrierungsanforderung 3
  auswerten 26
  automatisierte Auswertung 26
  Bearbeitung durch RA 3
  Registrierungsdatenbanksatz 28
  Registrierungsdomäne 27
  Registrierungsformular 25
  über Client-Anwendung 17
  über die Registrierungs-Web-Seite 5
  Verarbeitungszyklus 28
  Vorabregistrierung 25
  Web-Browser-Unterstützung 26
Registrierungsbeschränkungen 33
Registrierungsdatenbanksätze 3, 27, 28
  Attribute 28
  Bearbeitung durch RA 3
Registrierungsdomäne 27
Registrierungsformularfelder 33
Registrierungsstelle 3, 27

S

Schlüssel, beschädigt 37
Server-Zertifikat 7, 30
SHA1 With RSA, Algorithmus 46
Smart Card 16, 17, 31
  Eigenschaften 24
  Eigenschaften anzeigen 24
  eine andere verwenden 18
  eine physische Karte aktivieren 15
  Kennwort 23
  Kennwort ändern 23
  öffnen 23
  physische Karte 23, 31
  Verwaltung 23
  virtuelle Karte 16, 23, 31
  Zertifikat auf eine andere verschieben 19
  Zertifikat exportieren 18
  Zertifikat importieren 19
Smart Card, Fenster
  Dialoge 40
  Hilfefunktion 47
  mehr Zeilen in einer Tabelle anzeigen 22
  Menüs 39
  Registerkarten 22, 40
  Spaltengröße ändern 23
  Tabellen 40
  zwischen Registerkarten wechseln 22
Systemvoraussetzungen
  Browser-Registrierung 38
  Client-Anwendung 38

T

Tabelle
  mehr Zeilen anzeigen 22
  Spaltengröße ändern 23
Tabellen, Fenster 'Smart Card' 40
TACInst.exe, Datei 14
TAClient.ini, Datei 15
Transaktions-ID 17
Trust Authority, Zusammenfassung 1
Typ des Zertifikats 36

U

Übersicht 3
Unternehmensregeln 26
Unterschriftsalgorithmen 46
Unterzeichnen von Dateien 31
URL
  Registrierungs-Web-Seite 5
  Registrierungsdomäne 20, 27
  Registrierungsstelle 21

V

Verlassen der Client-Anwendung 24
Verwendungszweck des Zertifikats 36
Vorabregistrierung 25
  Anforderungsstatus überprüfen 10
  mit Transaktions-ID 17
  mit Vorabregistrierungsdatei 17
  Szenario für Tasks 25
Vorabregistrierungsdatei 10, 17

W

Wartestatus, Zertifikat
  über Client-Anwendung 20
Wartestatus, Zertifikat *(Forts.)*
  über die Registrierungs-Web-Seite 12
Web-Browser-Unterstützung 25, 26
Web-Seite, Registrierung 3, 5
  Anforderungs-ID 6, 7, 9
  Anforderungsstatus überprüfen 10
  CA-Zertifikat 29
  Felder des Registrierungsformulars 33
  Registrierungsarten 25
  Szenario für die Vorabregistrierung 25
  URL 5
  Zugriff 5
Widerruf
  Begründung 37
  über Client-Anwendung 21
  über die Registrierungs-Web-Seite 13

X

X.509v3-Zertifikatserweiterungen 30

Z

Zertifikat 29
  Anforderung über die Registrierungs-Web-Seite 5
  aus einer Datei importieren 19
  Datenbanksätze 27
  demnächst ablaufend 20, 41
  Details 19
  erneuerbar 30
  in eine Datei exportieren 18
  Kategorien 29
  löschen 18
  nicht erneuerbar 30
  Typen 36
  über Client-Anwendung anfordern 17
  über Client-Anwendung verwalten 18
  Verwaltung über die Registrierungs-Web-Seite 11
  zur Verwendung der Registrierungsservices 5, 29
  zusammenfassende Informationen 22
Zertifikatsaussteller (CA) 3, 28
Zertifikatserweiterungen 30
Zertifikatstypen 36
Zertifikatsverarbeitungszyklus 28, 30
Zertifikatsverwaltung (im Web) 11
  Anforderung für Browser 6
  Anforderung für Server-Einheit 7
  erneuern 12
  in den Wartestatus setzen 12
  Vorabregistrierung 9
  widerrufen 13
Zertifikatsverwaltung (über Client) 18
  Dateien unterzeichnen 21
  Details anzeigen 19
  erneuern 20
  in den Wartestatus setzen 20
  Liste anzeigen 22
  öffnen 19
  widerrufen 21

Zertifikatsverwaltung (über Client) 18
(Forts.)
Zertifikat auf eine andere Smart Card verschieben 19
Zertifikatswiderrufsliste (CRL) 28
Zertifizierung 28
gegenseitige Zertifizierung 28
Hierarchie 28
Zugriffssteuerungsliste (ACL) 31
Zusammenfassende Informationen, Zertifikate 22

Antwort

IBM SecureWay Trust Authority
Benutzerhandbuch
Version 3 Release 1.2

IBM Form SH12-2978-01

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen. Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre IBM Geschäftsstelle, Ihren IBM Geschäftspartner oder Ihren Händler.

Unsere Telefonauskunft ″HALLO IBM″ (Telefonnr.: 01803/31 32 33) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.

Kommentare:

Danke für Ihre Bemühungen.

Sie können ihre Kommentare betr. dieser Veröffentlichung wie folgt senden:
- Als Brief an die Postanschrift auf der Rückseite dieses Formulars
- Als E-Mail an die folgende Adresse: comment@tcvm.vnet.ibm.com

Name	Adresse
Firma oder Organisation	
Rufnummer	E-Mail-Adresse

Antwort
SH12-2978-01

IBM Deutschland Informationssysteme GmbH
SW NLS Center

70548 Stuttgart

Programmnummer: 5648-D09

Printed in Denmark

SH12-2978-01